

2 2 S C 0 9 0633 _ _

STATE OF SOUTH DAKOTA
VENDOR CONTRACT
BETWEEN

Metrc LLC
4151 South Pipkin Road
Lakeland, FL33811
(877) 566-6506

Referred to as "Vendor"

South Dakota Department of Health
600 East Capitol Avenue
Pierre, SD 57501-2536
(605) 773-3361

Referred to as "State"

State and Vendor hereby enter into a contract for project based professional services and modifiable off the shelf software.

I. VENDOR

- A. Grant of License. Subject to the terms and conditions of and except as otherwise set forth herewith, Vendor grants State a nontransferable and nonexclusive license to use, but not to relicense, sublicense, modify or enhance, the Metrc software system and related modules and user licenses.
- B. The term of this Contract shall begin March 15, 2022 and end March 14, 2027. The State of South Dakota retains three additional options to extend the contract period by one year each.
- C. Vendor is not a full or part-time employee of State or any agency of the state of South Dakota.
- D. Vendor, as an independent contractor, is solely responsible for the withholding and payment of applicable income and Social Security taxes due and owing from money received under this contract.
- E. Vendor will not be utilizing any equipment, supplies or facilities owned by the state of South Dakota.
- F. Vendor will not purchase capital assets or equipment using State funds.
- G. Vendor agrees to complete the activities and provide the services outlined in the Vendor's submitted proposal in response to the State's Request for Proposal #2439, which proposal is incorporated herein by reference as **Exhibit A**, with the exception of the following three (3) optional services described in Section IV.c on page 128 of the proposal: Lab Documents, Item Photos, and Item Approval Process.

H. **INSURANCE:** Vendor agrees, at its sole cost and expense, to maintain the following insurance:

1. **Commercial General Liability Insurance:**

Vendor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$1,000,000 each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this contract or be no less than two times the occurrence limit.

2. **Professional Liability Insurance:**

Vendor shall procure and maintain professional liability insurance with a limit of not less than one million dollars.

3. **Business Automobile Liability Insurance:**

Vendor shall maintain business automobile liability insurance or equivalent form with a limit of not less than \$1,000,000 each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles.

4. **Worker's Compensation Insurance:**

Vendor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

5. **Certificates of Insurance:**

Before beginning work under this Contract, Vendor shall furnish State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Contract. In the event of a substantial change in insurance, issuance of a new policy, cancellation or nonrenewal of the policy, Vendor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required. Vendor shall furnish copies of insurance policies if requested by State.

- I. Vendor agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as a result of Vendor's providing services or products under this Agreement. Vendor shall not be responsible for or required to defend against claims or damages arising from acts or omissions of the State, its officers, agents, or employees. Where Vendor is responsible for defending and indemnifying the State of South Dakota, Vendor has the right to control the defense any claims, suits, or other proceedings and shall have the right to select counsel related to such defense. The State of South Dakota shall cooperate in the defense of any and all such claims, suits or other proceedings.

- J. **NO IMPLIED CONVEYANCE OF PROPRIETARY RIGHTS.** State acknowledges that the Vendor Software represents and will continue to represent the valuable, confidential, and proprietary property of Vendor. Specifically, State acknowledges that aspects of the Vendor Software and associated documentation, including the training, specific design, and structure of individual programs, may be protected by Vendor's patent, copyright,

trademark, service mark, trade secret, trade name or other intellectual property rights (collectively, the "Intellectual Property Rights"). State shall not disclose, provide, or otherwise make available such Intellectual Property Rights in any form to any third party without the prior written consent of Vendor. Vendor is not by this Agreement conveying to State any of its Intellectual Property Rights in the Vendor Software.

State will not sell, license, sublicense, transfer or otherwise disclose or dispose of the Vendor Software or the Intellectual Property Rights or Confidential Information, or any portion thereof, and will take such precautions with respect to the Software and the Intellectual Property Rights and Confidential Information as are taken by State to protect its own confidential information and proprietary rights of the greatest sensitivity. State agrees that it will not make any corrections to or otherwise modify the Vendor Software or create derivative works based on the Vendor Software, or permit third parties to do the same, or decompile, decrypt, reverse engineer (including reverse engineering access to the database), disassemble or otherwise reduce the Vendor Software to human readable form to gain access to the Intellectual Property Rights in the Vendor Software or Confidential Information.

II. STATE

- A. State will pay, upon the State's satisfaction that the payments are in accordance with all items of the contract, up to \$375,000.00, which consists of \$55,000.00 in implementation costs, and \$320,000.00 in Software as a Service costs over a five-year period, as outlined in the Cost Proposal, described at Section V, Appendix B on pages 130 and 131 of Exhibit A. Vendor shall submit to the State invoices for payment upon the completion of the deliverables described at Section V, Appendix B, Paragraph 2, on page 131 of Exhibit A. State shall submit payment to the Vendor upon State's satisfaction as to the completion of the work subject to each invoice/the respective invoice. Vendor shall submit invoices on a monthly/quarterly basis to the State for payment of the yearly Software as a Service costs. Expenditure claims are required prior to the initiation of any and all payments. Expenditure claim documentation may include: invoices for reimbursement; receipts of any goods or services purchased; purchase orders for supplies, equipment, etc.; and/or itemized budget details indicating how and the timeframe in which the funds will be used.
- B. State will not pay Vendor expenses as a separate item.
- C. TOTAL CONTRACT AMOUNT (Not to Exceed) \$375,000.00. Payment will be made consistent with SDCL Ch. 5-26.
- D. Vendor agrees that the costs borne by medical cannabis establishment users will be limited to a \$480.00 annual fee per credentialed license and tag costs of \$0.45 per plant tag and \$0.25 per wholesale package tag plus related shipping and handling charges. Medical establishments will pay these costs to Vendor directly.

- E. State will not be held liable for reimbursement of amounts shown on an itemized billing if not received within 30 calendar days from the close of the month being reported. However, the final invoice of the State of South Dakota fiscal year, ending every year on June 30, shall be submitted no later than June 9 so payment may be made in the same Fiscal Year as the services are provided.
- F. Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software and services; telecommunication equipment, software and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions and other units of state government. BIT requires the contract provisions which are attached to this Agreement as **Exhibit B** and incorporated herein by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only **Exhibit B** of this agreement. Before renewal of this Agreement BIT must review and approve **Exhibit B** as still being current. BIT's evaluation of **Exhibit B** will be based on changes in the IT security or regulatory requirements. Changes to **Exhibit B** must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be provided to the Vendor with the understanding that the Vendor will adhere to the most current State IT security policies.
- G. Vendor agrees to the terms of the Security Acknowledgement form, incorporated into this agreement as **Exhibit C**.

III. OTHER PROVISIONS

- A. CHOICE OF LAW AND FORUM. The terms and conditions of this contract are subject to and will be construed under the laws of the State of South Dakota. The parties further agree that any dispute arising from the terms and conditions of this contract, which cannot be resolved by mutual agreement, will be tried in the Sixth Judicial Circuit Court, Hughes County, South Dakota.
- B. INTEGRATION. This contract is a complete version of the entire agreement between the parties with respect to the subject matter within this contract and supersedes all prior or contemporaneous written or oral understandings, agreements, and communications between them with respect to such subject matter. This contract may be modified or amended only by a writing signed by both parties.
- C. TERMINATION: This contract may be terminated for Cause by either party hereto upon thirty (30) days written notice, after a written notice of such has been delivered and the Party has been given ten (10) days to cure any identified issues under the Agreement. Either party may terminate this Agreement for convenience after a ninety (90) day written notice has been delivered. State shall pay Vendor for services under this contract received through the date of termination, as well as any services incurred to migrate the services to a new vendor or for the storage and retention of data held in the Vendor Software. Such service fee shall be mutually agreed upon by the Vendor and the State before any service is performed.
- D. NOTICE: Any notice or other communication required under this contract shall be in writing and sent to the address set forth above. Notices shall be given by and to the State Contact Person on behalf of State, and by and to the Vendor Contact Person on behalf of Vendor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

- E. **ASSURANCES:** The Vendor agrees to abide by all applicable provisions of the following assurances: Lobbying Activity, Byrd Anti Lobbying Amendment (31 USC 1352), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013, American Recovery and Reinvestment Act of 2009, and Section 106 (g) of the Trafficking Victims Protection Act of 2002, as amended (22 U.S.C. 7104) as applicable.
- F. **RESTRICTION OF BOYCOTT OF ISRAEL:** Pursuant Executive Order 2021-01, for contractors, vendors, supplies, or subcontracts with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars (\$100,000) or more, by signing this contract Vendor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of the contract, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for State to terminate this contract. Vendor further agrees to provide immediate written notice to State if during the term of the contract it no longer complies with this certification, and agrees such noncompliance may be grounds for contract termination.
- G. **CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:**
Vendor agrees that neither Vendor, nor any of Vendor's principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by any Federal department or agency. Vendor will provide immediate written notice to the Department of Health, Division of Administration (600 East Capitol Avenue, Pierre, SD 57501 (605) 773-3361), if Vendor, or any of Vendor's principals, becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions involving Federal funding. Vendor further agrees that if this contract involves federal funds or federally mandated compliance, then Vendor is in compliance with all applicable regulations pursuant to Executive Order 12549, including Debarment and Suspension and Participants' Responsibilities, 29 C.F.R. § 98.510 (1990).
- H. **FUNDING TERMINATION:** This contract depends upon the continued availability of appropriated funds and expenditure authority from Congress, the Legislature or the Executive Branch for this purpose. This contract will be terminated for cause by State if Congress, the Legislature or Executive Branch fails to appropriate funds, terminates funding or does not grant expenditure authority. Funding termination is not a default by State nor does it give rise to a claim against State.
- I. **NONASSIGNMENT/SUBCONTRACTING:** Vendor shall not assign this contract, or any portion thereof, without the prior written consent of State. Vendor's assignment or attempted assignment of this contract, or any portion thereof, without State's prior written consent constitutes a material breach of contract. The Vendor may not use subcontractors to perform the services described herein without the express prior written consent of State. Vendor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage in a manner consistent with this Agreement. Vendor will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.
- J. **FEDERAL AND STATE LAWS:** Vendor agrees that it will comply with all federal and state laws, rules and regulations as they may apply to the provision of services pursuant to this contract, including the Americans with Disabilities Act (ADA) of 1990, 42 U.S.C. §§ 12101-12213, and any amendment thereto, Section 306 of the Clean Air Act, and Section 508 of the Clean Water Act. Both parties further agree to provide services covered by this contract without regard to race, color, national origin, sex, age or disability as prohibited by state or federal law.
- K. **OWNERSHIP:** All reports, recommendations, documents, drawings, plans, and specifications tailored to the State and the services specific to the implementation of this contract, will become the sole property of State. State hereby grants Vendor the unrestricted right to retain copies of and use these materials and the information contained therein in the normal course of Vendor's business for any lawful purpose.

- L. **REPORTING OF PERSONAL INJURIES AND/OR PROPERTY DAMAGE:** Vendor agrees to report promptly to State any event encountered in the course of performance of this contract which results in injury to the person or property of third parties, or which may otherwise subject Vendor or State to liability. Reporting to State under this section does not satisfy Vendor's obligation to report any event to law enforcement or other entities as required by law.
- M. **SEVERABILITY:** In the event that any term or provision of this contract shall violate any applicable law, such provision does not invalidate any other provision hereof.

N. **AUDIT REQUIREMENTS:**
(EXPENDING \$750,000 OR MORE)


A nonprofit subrecipient, (as well as profit hospitals) (Vendor), expending \$750,000 or more in one year in Federal awards, must have an annual audit made in accordance with 2 CFR Chapter I, Chapter II, Part 200, et al. Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.

All audits must be conducted by an auditor approved by the Auditor General to perform the audit. Approval may be obtained by forwarding a copy of the audit engagement letter to the Department of Legislative Audit, 427 South Chapelle, c/o 500 East Capitol, Pierre, SD 57501-5070. On continuing engagements, the Auditor General's approval should be obtained annually. The auditor must follow the Auditor General's guidelines when conducting the audit. The draft audit report must be submitted to the Auditor General for approval prior to issuing the final report. The auditor must file the requested copies of the final audit report with the Auditor General. Audits shall be completed and filed with granting agencies by the end of the ninth month following the end of the fiscal year being audited or 30 days after receipt of the auditor's report, whichever is earlier. If it appears that a required audit cannot be completed by the end of the ninth month following your fiscal year, you must request an extension from the federal agency for which the majority of federal expenditures relates.

Failure to complete audit(s) as required will result in the disallowance of audit costs as direct or indirect charges to programs. Additionally, a percentage of awards may be withheld, overhead costs may be disallowed, and/or awards may be suspended, until the audit is completed satisfactorily.

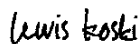
- O. **FORCE MAJEURE:** Neither Vendor nor State shall be liable to the other for any delay in, or failure of performance of, any covenant or promise contained in this contract, nor shall any delay or failure constitute default or give rise to any liability for damages if, and only to the extent that, such delay or failure is caused by "force majeure". As used in this contract, "force majeure" means acts of God, acts of the public enemy, acts of the State and any governmental entity in its sovereign capacity, fires, floods, epidemics, quarantine restrictions, strikes or other labor disputes, freight embargoes, or unusually severe weather, including hurricanes.
- P. **CONTRACT ORIGINAL AND COPIES:** An original of this contract will be retained by the State Auditor's Office. A photocopy will be on file with the South Dakota Department of Health and a second original will be sent to Vendor.
- Q. **RECORD RETENTION/EXAMINATION:** Vendor agrees to maintain all records that are pertinent to this contract and retain them for a period of three years following final payment against the contract. State agrees to assume responsibility for these items after that time period. These records shall be subject at all reasonable times for inspection, review or audit by State, other personnel duly authorized by State, and federal officials so authorized by law.
- R. **LICENSING AND COMPLIANCE:** The Vendor agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this agreement. The Vendor will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Vendor's failure to ensure the safety of all individuals served is assumed entirely by the Vendor.
- S. **Reserved.**
- T. **CONFLICT OF INTEREST:** Provider agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Provider expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.
- U. **RECYCLING.** State strongly encourages Vendor to establish a recycling program to help preserve our natural resources and reduce the need for additional landfill space.

In WITNESS WHEREOF, the parties have indicated their acceptance of the terms of this Agreement by their signatures below.

DocuSigned by:

 Lynne Valenti, Deputy Secretary
 Division of Healthcare Access &
 Quality and Health Protection
 Department of Health

3/21/2022

Date

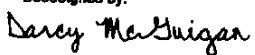
DocuSigned by:

 Consultant Signature

3/18/2022

Date

Lewis Koski

Print or Type Vendor Name

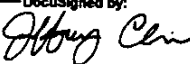
DocuSigned by:

 Darcy McGuigan, Director
 Division of Finance
 Department of Health

3/21/2022

Date

Lewis.Koski@metrc.com

Vendor e-mail address

DocuSigned by:

 Jeff Clines, Commissioner
 Bureau of Information & Telecommunications
Approval as to Exhibit B only

3/21/2022

Date

State Contact Person: Geno Adams Phone: 605-773-6697

Vendor Contact Person: Lewis Koski Phone: 3034348550

The following shall be completed by the Vendor:

Nonprofit ☐ Profit ☐

Vendor fiscal year beginning Jan. and ending Dec.

The following shall be completed by the State:

MSA Account code 5 2 0 4

Fund Source Name:	Fund Source Name:	Fund Source Name:
CFDA No:	CFDA No:	CFDA No:
Program: 0903007-	Program: 0901001-	Program: 0901001-
CO: 2018-Federal \$375,000.00	CO: 2018-Federal	CO: 2018-Federal
3047-Other	3047-Other	3047-Other
1000-General	1000-General	1000-General

SDCL 1-24A-1 states that a copy of all consulting contracts shall be filed by the agency with the State Auditor within five days after such contract is entered into and finally approved by the contracting parties. For further information about consulting contracts, see the State Auditor's policy handbook.

Seed to Sale Tracking System for the State of South Dakota Department of Health and Department of Revenue



RFP # 2439
August 23, 2021



**Metrc Response to RFP # 2439
August 23, 2021**

**Request for Proposal to Develop and Implement the South Dakota Cannabis
Seed to Sale Tracking System for the State of South Dakota
Department of Health and Department of Revenue**

Submitted to:

Sakura Rohleder, Buyer

Email: Sakura.Rohleder@state.sd.us

Submitted by:

Metrc LLC

4151 South Pipkin Road

Lakeland, Florida 33811

Proposal Contact: Cindy Register, Proposal Manager

Phone: (864) 380-3431

Email: Cindy.Register@Metrc.com



August 23, 2021

Ms. Sakura Rohleder, State of South Dakota
Department of Health and Department of Revenue
455 E. Capitol Avenue
Pierre, South Dakota
Ref: RFP # 2439

Dear Ms. Rohleder,

The requirements that the State of South Dakota (State) is seeking to address with its Cannabis Seed to Sale Tracking System are a perfect match with the system and services Metrc LLC (Metrc) delivers in 16 other state jurisdictions. We appreciate this opportunity to respond to your Request for Proposal and present you with a proven, seed-to-sale tracking system. We are confident that our solution will fully meet the requirements and expectations of both the Department of Health and Department of Revenue. We applaud the State for your continued commitment to tracking plants and products from seed to sale in accordance with South Dakota code SDCL Ch. 24-20G.

We have thoughtfully evaluated and prepared our response to ensure we provide the State with the highest-quality solution at the lowest possible cost and with minimal impact to the regulated community. As you will see in our response, Metrc's system meets the RFP requirements for the seed to sale tracking system. Our prior experience and exclusive focus on regulatory cannabis software means that South Dakota will benefit from a mature system. Historically, we have met 90% of customer requirements out of the box with only minor configuration needed for the remaining 10% of the requirements. As you will see in our proposal, we will meet 100% of the State's requirements in our implementation.

Metrc makes every resource available to ensure a safe and effective medical and, if approved, adult-use cannabis market. Metrc's intent is to support the State's mission to assist, educate, and protect the public.

Again, we appreciate the opportunity to describe our approach in the attached proposal and look forward to including South Dakota with the other valued clients we currently serve.

Should you have any questions about Metrc's proposal, please contact Cindy Register by phone at (864) 380-3431 or email at cindy.register@metrc.com.

Metrc certifies our agreement to the requirements and information contained in the RFP.

Sincerely,

A handwritten signature in black ink that reads "W. 'Lewis' Koski".

W. "Lewis" Koski
Metrc LLC Chief Operations Officer



Table of Contents

I.	RFP Form	5
II.	Executive Summary	6
III.	Response to Software Requirement.....	8
IV.	Detailed Response	21
IV.a.	Narrative of Metrc's Assessment of Work to be Performed	21
IV.a.1.	Approach and Methodology to Meet Project Requirements	22
IV.a.2.	Resources to Fulfill Requirements	30
IV.a.3.	Record of Past Performance	35
IV.a.4.	Availability and Familiarity with Project Locale	37
IV.a.5.	Project Management Techniques.....	37
IV.a.6.	Ability and Proven History in Handling Special Project Constraints	41
IV.b.	Response to Software Requirements	43
IV.b.1.	Cultivator and Manufacturer Tracking and Inventory	43
IV.b.2.	Dispensary Tracking and Inventory	67
IV.b.3.	Tracking and Inventory Audit and Enforcement.....	72
IV.b.4.	Security & Maintenance	78
IV.b.5.	Operation.....	112
IV.c.	Options or Alternatives Proposed	128
V.	Cost Proposal.....	130
VI.	Metrc Hosted Security and Vendor Questions (Appendix D)	137
VII.	List of Subcontractors.....	138
VIII.	Statement of Understanding of the Project	139
IX.	Additional Forms/Appendices	141



I. RFP Form

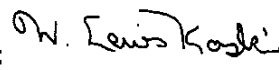
STATE OF SOUTH DAKOTA
DEPARTMENT OF HEALTH and DEPARTMENT OF REVENUE
455 E CAPITOL AVENUE
PIERRE, SOUTH DAKOTA 57501

REQUEST FOR PROPOSAL TO DEVELOP AND IMPLEMENT THE SOUTH DAKOTA
CANNABIS SEED TO SALE TRACKING SYSTEM
PROPOSALS ARE DUE NO LATER THAN 5:00 PM CDT AUGUST 23, 2021

RFP #2439 BUYER: Sakura Rohleder EMAIL: Sakura.Rohleder@state.sd.us

READ CAREFULLY

FIRM NAME: Metrc LLC

AUTHORIZED SIGNATURE: 

ADDRESS: 4151 S. Pipkin Road

TYPE OR PRINT NAME: Lewis Koski, Metrc COO

CITY/STATE: Lakeland, Florida

TELEPHONE NO: 877-566-6506

ZIP (9 DIGITS): 33811-1425

FAX NO: 863-577-0955

E-MAIL: Lewis.Koski@Metrc.com

PRIMARY CONTACT INFORMATION

CONTACT NAME: Cindy Register

TELEPHONE NO: 864-380-3431

FAX NO:

EMAIL: Cindy.Register@Metrc.com



II. Executive Summary

Metrc is pleased to respond to the State of South Dakota's (the State) Request for Proposal for a Cannabis Seed-to-Sale Tracking System. We understand that the system is being procured by the Department of Health on behalf of both itself and the Department of Revenue for the medical and possible adult-use markets, respectively.

If the State chooses to work with Metrc LLC (Metrc), you will be selecting a vendor who has more cannabis track-and-trace experience than any other and who is focused exclusively on serving regulators in the cannabis market. The State will also be selecting an enterprise solution that includes Software as a Service (SaaS) along with service management and training and support for users and licensees. Metrc's software tracking system (Metrc System, the System) is robust, secure, highly configurable, and fully deployable within six months. Metrc's dedication to our partners' success is proven by the fact that every agency that has selected Metrc as their track-and-trace vendor has repeatedly extended our relationship because we continually meet and exceed their objectives.

The following differentiators elaborate further on the benefits the State will experience through a partnership with Metrc:

- **Aligned Priorities – The State's interests are Metrc's focus.** Metrc's only product is regulatory software—we're not focused on upselling other products, such as consulting services or point of sale software, to industry.
- **Experience – Current contracts with 16 jurisdictions, 100% contract renewal rate.** Metrc has more state contracts than any other track-and-trace vendor and is currently the only vendor to fully expand a track-and-trace system from a medical to an adult-use market.
- **Service – The State will receive unlimited support and training and access to senior leadership.** The State will have direct access to an assigned contract manager and senior leadership. The State and licensee users will receive unlimited, high-quality support and training that includes in-person and online courses.
- **Affordability – The State will save money.** The State's costs are minimized because Metrc bears the capital cost to implement the System to include reasonable system enhancements at no additional cost to the State.
- **Flexibility – The System will deliver the State's desired functionality and be highly configurable.** Metrc currently meets—or will be able to meet—100% of the State's software requirements, as further detailed in this proposal. Furthermore, since our System is highly adaptive, new requirements can be quickly addressed to keep pace with changing policy, rule, or law.

Major Features

Metrc has the experience to provide the system and services the State seeks. Metrc is the leading provider of track-and-trace solutions, with 10 years of experience partnering with public sector clients in the cannabis industry. The following details attest to our expertise:



- The State of Colorado partnered with Metrc in 2011 to develop the first statewide track-and-trace system for marijuana; 15 other jurisdictions have partnered with us since then.
- Metrc's proprietary tags use RFID chip, a barcode, and a human-readable unique number identifier (Hex-ID) to track marijuana through every phase of the supply chain in real time.
- In the jurisdictions we serve, Metrc has over 1,400 regulatory users and 240,000 licensee users from over 30,000 licensed businesses.
- Our regulatory clients have used the Metrc System to track almost \$24 billion in sales and over 1 billion supply chain events.

Our proposal also demonstrates how prepared Metrc is to deliver the cultivator, manufacturer, and dispensary tracking and inventory capabilities; the audit and enforcement tracking and inventory capabilities; the security and maintenance; and the operations that the State requires to implement a successful seed-to-sale tracking program. Our proven software, processes, and people will exceed the State's goals by capturing cannabis plant and product data throughout the supply chain, from cultivation, transportation, processing, testing, and dispensing.

Furthermore, our proposal details the System's demonstrated ability to integrate with other systems. In addition to our experience integrating with various agency systems (such as patient registries and licensing systems) in each of our contracts, there are over 500 third-party, industry-serving software providers that integrate into our System.

Ultimately, the State will receive a fully functional system that meets its technical requirements, an on-time and well-managed implementation executed by a team with robust cannabis-industry expertise, a comprehensive training and support program for all users, and hands-on support to ensure your System continues to meet changing needs over the lifetime of our contract.

Requirements That Can't be Met

Metrc's System can meet all RFP requirements.

Proprietary Information Requests

Metrc requests that the following documents be kept confidential from public disclosure. Release of such information would reveal security, including cybersecurity, of the design, construction, and operation of the network and associated services and products. The documents include the following: Appendix D – Metrc Hosted Security and Vendor Questions; Attachment 6 – Business Continuity & Disaster Recovery Plan; and Attachment 7 – System Security Plan; Attachment 8 – Security and System Architecture.

The State's success is paramount, and we will make every possible resource available to ensure that we deliver a system and services that help the State achieve and exceed its goals and objectives. Thank you for your consideration and the opportunity to serve South Dakota, and the State's future medical marijuana and adult-use consumers.



III. Response to Software Requirement

The following requirements table includes page references where each requirement is addressed within the proposal. Metrc will meet 69/69 of the State's software requirements.

Cultivator and Manufacturer Tracking and Inventory (proposal section IV.b.1)				
ID	CATEGORY	REQUIREMENT	YES/ NO	PAGE REF. IN PROPOSAL
3.1a	Inventory Information Tracking	The system must provide cultivators and manufacturers the ability to define inventory of plants, strains, clones, seedlings, and cannabis product. The information that must be tracked in the system are including but not limited to the following: <ul style="list-style-type: none"> • Unique identifiers for individual plant; • Quantity and form of cannabis maintained by the establishment at the facility in the appropriate units of measure determined by the State; • The amount of plants being grown at the facility; • The amount of plants being processed at the facility; and • Any other information required by the State The inventory record must reflect destruction or disposal of cannabis waste, theft, and transfer record. 	YES	43
3.1b	Inventory Record Updates - Cultivator	The system must allow the inventory record to be updated each time: <ol style="list-style-type: none"> 1. A seedling exceeds its size limit determined by the State and is considered a plant; 2. A plant flowers for the first time; 3. A plant is trimmed or harvested; 4. A testing batch is created; or 5. Cannabis is packaged for retail sale. The record of cannabis packaged and labeled for transfer must include the number of marketing layer, and quantity of cannabis in each marketing layer. 	YES	48
3.1c	Inventory Record Updates - Manufacturer	The system must allow the inventory record to be updated each time: <ol style="list-style-type: none"> 1. A quantity of extract or concentrated cannabis is made from cannabis flower or trim; 2. A quantity of cannabis product is made from concentrated cannabis, cannabis extract, flower, or trim; 3. A quantity of cannabis product is packaged for retail sale. The record of cannabis packaged and labeled for transfer must include the number of marketing layer, and quantity of cannabis in each marketing layer.	YES	49
3.1d	Inventory Record	The system must maintain and update an electronic copy of the following information:	YES	50



Cultivator and Manufacturer Tracking and Inventory (proposed section 4(b.1))				
	Updates - Testing Facility	<p>1. All samples in its possession with unique identifiers and quantities expressed in units specified by the State; and</p> <p>2. All other cannabis, cannabis extracts, and cannabis products acquired</p> <p>The inventory record should reflect:</p> <ul style="list-style-type: none"> • The quantity of each sample rendered unusable by testing; • The quantity of each sample returned to the establishment; • The quantity of each sample destroyed or disposed of; and • The quantity of any sample lost, stolen, or otherwise unaccounted for. 		
3.1e	Inventory Reconciliation	<p>Cannabis Establishments will reconcile their physical inventory with the information in the system at the end of business each day. Inconsistencies will flag the department for further investigation. Reconciliation items will include the following:</p> <ul style="list-style-type: none"> • Plant material at the facility; • Plant material in transit; and • Any other information required by the State 	YES	51
3.1f	Daily Transfer Record	<p>The system must maintain and update by midnight an electronic record of all cannabis including seeds, plants extracts, or products obtained by a cardholder or another establishment, and all cannabis transferred to another establishment. The transfer record must meet the following requirement:</p> <ol style="list-style-type: none"> 1. It must use the same units of measures as the inventory record; and 2. It must reflect all transport manifest, purchase orders, and requisition forms. 	YES	52
3.1g	Pesticides Tracking	<p>The system must provide the establishment the ability to track and any pesticides used during production. The following items will be recorded in the system:</p> <ul style="list-style-type: none"> • The date of pesticides being applied; • The name of the employee applying the pesticides; • The name of pesticides that was applied; • The amount of pesticides applied; • The unique identifier or the batch number of plants that received the application; and • A copy of the label of the pesticides applied 	YES	53
3.1h	Lab Testing	<p>The system must be able to track sample procurement, sample origin, testing stages, testing results, and alert the State upon testing failure. The system must be able to record all of the following attributes of any plant or product: Cannabinoid Potency; Microbials; Heavy metals; Solvents;</p>	YES	54



Cultivator and Manufacturer Tracking and Inventory (proposal section IV.b.1)				
		<p>Pesticides; and Any other attributes required for testing by Administrative Rules</p> <p>The testing results and record can only be added by an agent of testing facility, and the record should not be editable by agents of other establishment types.</p>		
3.1i	Testing Sample Record	<p>The system must allow establishments to assign the following identifier to samples being submitted to the testing facility:</p> <ol style="list-style-type: none"> 1. A unique batch identifier to the cannabis, cannabis extract, or cannabis product being tested; and 2. A unique sample identifier to each sample unless the sample is taken by an agent of the testing facility. <p>The system must allow establishment to maintain an electronic copy of testing sample record that includes the following information:</p> <ul style="list-style-type: none"> • The batch identifier and quantity of each batch from which samples were drawn; • The identifier of each sample record, its quantity, and the batch identifier associated with the sample; • The tests to be performed; • Test results, including a note of whether the testing facility has indicated the batch is safe or unsafe for transfer; and • The quantity of each batch and each sample shall be expressed in the same units as the inventory record. <p>The System must alert the State upon testing failure or products not meeting the standards set by the State.</p>	YES	56
3.1j	Tracking and Disposal of Product	<p>The system must allow cultivator or manufacturer to record disposal of unused, excess, or expired cannabis including returned cannabis products from dispensaries or Cannabis cardholder.</p> <p>The system also must record the disposal of cannabis product that failed to meet testing standards. The system must provide abilities to record, reconcile and maintain the following information:</p> <ul style="list-style-type: none"> • The original tracking number at the time of the dispensing or the name of the patient if the tracking number is unavailable; • The date the cannabis was returned or disposed; • The quantity of cannabis returned or disposed; • The type and lot number of the cannabis returned or disposed; • Reason for disposal or return; • Any other information required by the State The system must flag any inconsistencies or unreconciled record of returned or disposed cannabis product. 	YES	57



Cultivator and Manufacturer Testing and Inventory (proposal section 3.1k)				
3.1k	Travel Manifest	<p>The cultivator and manufacturer are required to generate transport manifest for transportation of cannabis to and from their facility, dispensaries, testing facility, a waste facility, and other location as approved by the department.</p> <p>The system must record and issue the travel manifest and generate copies of the manifest. The travel manifest should contain the following information:</p> <ul style="list-style-type: none"> • The information of establishment transporting cannabis or cannabis products including but not limited to license number; • The information of establishment receiving cannabis or cannabis products including but not limited to physical address; • Web address of the departments' secure verification system; • Description and quantities of all items in each transport; • Date of transport, and approximate time of departure and arrival date; • Vehicle make, model and license plate number; • The name and signature of driver; • The name and signature of the establishment agent accepting the transport; • Any other information required by State 	YES	58
3.1l	Product Delivery Receipt	The system must provide an ability for establishment to record the cannabis that is received as inventory.	YES	59
3.1m	Sales and Distribution Record	<p>The cultivator and manufacturer will maintain complete and accurate electronic sales transaction records in the department's tracking system, including the following item;</p> <ol style="list-style-type: none"> 1. The date of each sale and distribution; <ul style="list-style-type: none"> • The item number, product name and description, and quantity of cannabis sold or otherwise distributed; • The sale price; and • Any other information required by the State 	YES	60
3.1n	Recall Mechanism for Manufacturer	Manufacturer may need to recall cannabis. The system should provide a mechanism to document any recalled product, reason for recall, date of recall, and relevant unique identifier for the batch or lot numbers. The system should also flag the State personnel for any recall actions taken by manufacturers within the system.	YES	60
3.1o	Requisition Form	The system must create a requisition form when a cultivation facility accepts cannabis from a cardholder at no value. The form must contain the cardholder's identification number and acknowledgement signature from cardholder that nothing of value was received in exchange of the cannabis.	YES	61



Cultivator and Manufacturer Tracking and Inventory (proposal section IV.b.1)				
3.1p	Purchase Order	The system must create a purchase order when a cultivation facility purchase seeds from a cardholder. The form must contain cardholder' s identification number, quantity of the seeds, value exchanged, and the acknowledgement signature from the cardholder.	YES	61
3.1q	Travel Manifest Approval (OPTIONAL)	Each transport should be approved electronically or in writing by an authorized employee of the establishments when departing the facility and by an authorized employee of the receiving establishment or waste facility. The system must allow authorized employees of the receiving establishment to review and verify the type and quantity of the transported cannabis or plant material against the information on the travel manifest prior to signing the travel manifest. If the approval process is in writing, the system should have the document upload functionality so the copy of the approved travel manifest is uploaded into the system.	YES	62
3.1r	In-Transit Documentation (OPTIONAL)	The system should have the ability for establishment agents who are transporting cannabis on public roads to record the following information: 1. Travel routes taken to deliver products to establishments; 2. Refueling and all other stops in transit, including reason, duration, and location of the stop. 3. Any traffic stop, breakdown, or collision involving a vehicle being used by an establishment to transport cannabis or cannabis product. 4. Any theft or break-in involving a vehicle being used by the establishments to transport cannabis or cannabis product.	YES	63
3.1s	Product Labeling (OPTIONAL)	The system should allow the manufacturer to create and print labels for the cannabis products. The label must include: • List of any pesticides used in cultivation; • List of all ingredients and any gases, solvents, or other chemicals used in extraction; • List of major allergens including milk, egg, fish, crustacean shellfish, tree nuts, peanuts, and soybeans; • Net weight or volume of the cannabis or cannabis product • Equivalent cannabis weight (See Requirement 3.1v) • The length of time that it may take the patient to feel effects; • The length of time the patient should expect the result to last; • The weight label must have the flexibility for unit size (serving size, weight of concentrate...etc.) based on the product type; • Nutritional fact panel;	YES	63



Cultivator and Manufacturer Tracking and Reporting (Optional Cannabis Seed)				
		<ul style="list-style-type: none"> Any symbol developed by State to indicate the availability of THC; Warning statement in font no smaller than 6 point font, "For use by qualifying patients only"; and Any other information required by the State <p>Additionally, the following test results can be listed on the label if the test was performed by registered cannabis testing facility: Absence of Microbials; Absence of heavy metals; Absence of solvents; Absence of pesticides; and Potency</p> <p>The font size for the label shall be no smaller than 6 point font (1/12 inch).</p>		
3.1t	Additives, Solvent, and Chemical Tracking (OPTIONAL)	<p>The system should provide the establishment the ability to track any additives, solvents, and other chemicals used during production. The following items will be recorded in the system:</p> <ul style="list-style-type: none"> The date of additives, solvent, or chemicals being applied; The name of the employee applying the additives, solvent, or chemicals; The name of additives, solvent, or chemicals that was applied; The amount of additives, solvent, or chemicals applied; The unique identifier or the batch number of plants that received the application; and A copy of the label of the additives, solvent, or chemicals applied 	YES	65
3.1u	Quality Assurance (OPTIONAL)	The system should allow manufacturer to record all quality control procedures, and outcomes by batch and lot number in the system.	YES	65
3.1v	Equivalent Dosage (OPTIONAL)	The system should be able to calculate equivalent dosages based on the equivalency table provided by the State.	YES	65
3.1w	Establishment Room Designation and Configuration (OPTIONAL)	The system should provide the establishments the ability to track plants through each growth phase by associating the individual plants with a particular room. Batches and partial batches will be tracked in the system. The cultivator and manufacturer will record any removal of plants from a batch including the reason for removal. The system must provide cultivators and manufacturers the ability to define and designate growing and production rooms. Rooms are including but not limited to the following: Germination; Vegetative; Flowering; Trimming; Curing; Processing; Packaging; Extraction; and Storage	YES	66



Dispensary Tracking and Inventory (proposal section IV.b.2)				
ID	CATEGORY	REQUIREMENT	YES/ NO	PAGE REF. IN PROPOSAL
3.2a	Inventory Record Updates - Dispensary	<p>The system must maintain and update an electronic copy of all cannabis and cannabis products including the type of products, testing batch identifier, the number of marketing layers, and the quantity of cannabis in each marketing layer. The inventory record should reflect:</p> <ol style="list-style-type: none"> 1. Any cannabis and cannabis products received from another establishments; 2. Sales to qualifying cardholders including the cardholder's identification number; 3. Returns of merchandise from cardholders, whether to be resold, returned to another establishment, or destroyed; 4. Transfers to another establishment including returns; and 5. Destruction of cannabis 	YES	67
3.2b	Tracking Number Assignment	The system must assign a tracking number to any cannabis that is to be dispensed to the patient or caregiver	YES	69
3.2c	Product Return to Manufacturer	<p>Dispensaries will record information on all cannabis collected by the manufacturers. The system must allow dispensaries to record the following information for product returns:</p> <ul style="list-style-type: none"> • The date of return; • The identification number for patient or caregiver if patient or caregiver returns the product to dispensary; • The number of marketing layers; • The quantity of the cannabis in each marketing layer; • The type of product; • Testing batch number of cannabis collected; and • Any other information required by the State <p>The system must flag any inconsistencies or unreconciled record of returned or disposed cannabis product.</p>	YES	69
3.2d	Dispensary Sales Record	<p>The system must require dispensaries to maintain complete and accurate sales transaction records including:</p> <ul style="list-style-type: none"> • The date of sale; • The cannabis tracking number; • The number of marketing layers; • The amount of cannabis or cannabis product dispensed; • The quantity of the cannabis in each marketing layer; • The type of product; • Testing batch number of cannabis sold; • The identification number for patient or caregiver if purchase was done by a caregiver; 	YES	70



Dispensary Tracking and Inventory Audit and Enforcement (proposed section IV A 3)				
		<ul style="list-style-type: none"> • The item number, product name , and description of items sold; • The sale price; and • Any other information required by the State 		
3.2e	Dispensary Inventory Reconciliation	The system must require dispensaries to reconcile all cannabis at the facility at the end of the business day against the sales and inventory tracking system. Inconsistencies will be flagged for the State personnel for investigation.	YES	70
3.2f	Dispensary Label Issuance (OPTIONAL)	The system should issue a label with the following information: <ul style="list-style-type: none"> • The medical cannabis tracking number; • The date and time the medication is being dispensed; • The name and address of the dispensary; • The patient's or caregiver's registry identification number; • Any specific instruction for use based on manufacturer or department guidelines; and • Any other information required by DOH 	YES	71

Tracking and Inventory Audit and Enforcement (proposed section IV A 3)				
ID	CATEGORY	REQUIREMENT	YES NO	GRADE IN PROPOSAL
3.3a	Vehicle Information	The establishments must be able to provide the following information to the department via this system regarding each vehicle that will be used to transport cannabis products: <ol style="list-style-type: none"> 1. Make, Model, and license plate number; 2. Proof of a valid insurance policy; 3. A description with photos of a locking compartment to be used to secure cannabis and cannabis products 4. Verification that the vehicle has a functioning alarm system; and 5. A description of how the cannabis and cannabis products will be maintained in a vehicle 	YES	72
3.3b	Internal Review	The system must provide the State personnel to review all establishment records as needed.	YES	72
3.3c	Internal Dashboard	The system must provide a dashboard where the State personnel can review all flags of inconsistencies and irregularities in the cultivation, production, manufacturing, transporting, dispensing, and disposal of cannabis or plant material.	YES	72
3.3d	Tracking Reporting	The system must have reporting functionality with easy-to-use query function. The system must have reporting tool with sort and filter function, an ability to save and share custom report	YES	73



Tracking and Inventory Audit and Enforcement (proposal section IV.b.3)				
		<p>specification, and an ability to export the report in various formatting including Microsoft Excel or PDF.</p> <p>The system should also come with template of reports including but not limited to the following:</p> <ul style="list-style-type: none"> • Total number of internal flags by reasons; • Breakdown of reasons for products that failed to meet testing standards; • Price report by product type; • Volume of sales by date range by individual establishment; • Tax Collection Report by establishment ID; • Breakdown of product purchased; and • List of product and its price sold at individual establishment 		
3.3e	Audit Logs	All actions by all users in the system should be tracked in an audit log including, but not limited to, username, action completed, and date/time stamp. When a user deletes information, the deletion is a "soft" delete and the data are not removed from the system and instead are still viewable to authorized personnel based on role-based security.	YES	74
3.3f	Communication to Establishments	The system must provide an ability for the State personnel to set alerts and notifications. The system should provide automatic alerts or reminders based on system rules. Alerts may be set based on programmatic business rules, workflow process, or initiated by an authorized user. Alerts may be system-wide, program, or user specific.	YES	75
3.3g	Data Integration	<p>The system must have an ability to integrate with the following systems:</p> <ol style="list-style-type: none"> 1. Cannabis Patient Registry; 2. Cannabis Business Licensing System; and 3. Point of Sale System 	YES	75
3.3h	Agent ID Login	Only the Cannabis Agent registered with the state can enter certain information in the system. The system should incorporate the integrated data from Cannabis Business Licensing System for log in to ensure that appropriate personnel at establishments are entering the information.	YES	76
3.3i	Data Validation	The system must have data validation function to prevent missing data or data type errors.	YES	77
3.3j	Data Retention	Unless otherwise stated in Administrative Rules, all data in the system must be maintained for a minimum of 10 years.	YES	77



Security and Access Management (Proposed Section 3.4)				
ID	CATEGORY	REQUIREMENT	YES/NO	FACTORY IN PROPOSAL
3.4a	State Single Sign on	As part of the State's Identity and Access Management (IAM) strategy, the proposed system must integrate with the State of South Dakota's standard identity management service (SSO) which enables custom control of how citizens and/or state employees sign up, sign in, and manage their profiles. The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0. This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users. <u>If the vendor is not able to fulfil this identity management standard, they will be considered disqualified and the proposal will not be evaluated.</u>	YES	78
3.4b	Patient Identification Method	The system shall not identify any cardholder other than by the cardholder's identification number assigned by patient registry system.	YES	78
3.4c	Hosting and Data Access	The vendor must agree that the State will own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms. The State will give preference to vendors who can provide a cloud-based solution hosted/deployed onto the States' Microsoft Azure Cloud Tenant or a States preferred platform.	YES	78
3.4d	Data Hosting Option	The vendor must host the solution, and the proposal must include the current server/system, specifications, software, and versions.	YES	79
3.4e	Web-based services	The system must have secure web-based access. The system must be accessible through various internet browser including Mozilla Firefox, Google Chrome, and Microsoft Edge. The system must also be mobile friendly.	YES	80
3.4f	System Upgrades	The proposal must include system upgrade plan that includes but not limited to upgrade plan, types and frequency of upgrades. The purpose of this plan is to ensure that the proposed solution(s) have upgrade procedures that creates minimal impact or interference on system availability.	YES	80
3.4g	System Issue Communication	The system must have an alert system where both external and internal users receive notification in case of system outage or issues with API in real time with estimated time needed for repair. The system must clearly communicate to all users when the issue is resolved.	YES	81



Security & Maintenance (proposal section IV.b.4)				
3.4h	System Maintenance	The system must have a periodic maintenance to update the system, fix any known issues, and address requested improvements.	YES	81
3.4i	Data Security	The data security for the proposed solution (s) must meet the requirements set by the State and HIPPA.	YES	82
3.4j	User Role Permissions	User Roles must limit CRUD (Create, Read, Update, Delete) access per Role. Addition of new Roles and changes to Role CRUD access must be easy.	YES	83
3.4k	Data Encryption	The system must utilize data encryption when data is sent	YES	84
3.4l	Sensitive Data Storing	The system must not store authentication credentials or sensitive data in its code.	YES	85
3.4m	Interfaces	The vendor must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, the State expects that the vendor will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the Proposal.	YES	86
3.4n	Data normalization	The system will have the ability of data normalization to reduce and eliminate data redundancy.	YES	87
3.4o	Design Pattern	The system permissions will follow an "explicitly granted" design pattern.	YES	87
3.4p	Environment	The system will require close/separate environments for: development, testing and production	YES	88
3.4q	Session Timeouts	The system will enforce session timeouts during periods of inactivity.	YES	88
3.4r	Credential Storing	The system will not store authentication credentials or sensitive data in its code.	YES	88
3.4s	Change Management Documentation	The system will utilize change management documentation and procedures.	YES	89
3.4t	Customer Support	The vendor must provide technical and end-user support via phone and email between 7:00 AM and 9:00 PM CT, 7 days per week. Additionally, the vendor must be available and has ability to respond to critical issues in timely fashion regardless of the time of the incident. The detail of disaster recovery and support requirements are outlined in the Appendix C, Section 9.2 (page 32).	YES	90
3.4u	Support and Maintenance Plan	The proposal must include system update plan. The plan at minimum must include the following items: 1. Testing: Provide the testing plan that describes a plan for user acceptance training, development of user acceptance	YES	94



Security & Reliability (proposed section IV 3.4)				
		<p>testing environment, stress regression, and performance test plan.</p> <p>2. Implementation: Provide the implementation plan of the application that describes how the implementation is prioritized, planned, managed, and executed.</p> <p>3. Ongoing Maintenance: Provide maintenance plan that describe level of support service provided with estimated response time.</p> <p>4. Modification: Provide methodologies for how modifications are charged to the State.</p>		
3.4v	Point of Sale (POS)	<p>The system must be able to integrate with point of sale system via an Application Program Interface (API) to ensure all data required by the State is recorded in system. The system must accept all major credit cards as well as payment via cash or check.</p> <p><u>The proposal must include the list of all POS systems that the system has successfully integrated.</u></p>	YES	65
3.4w	Integration Plan	<p>Integration plan, timeline, and previous integration experiences with the list of vendors/system must be submitted for the following system:</p> <ul style="list-style-type: none"> • Patient registry, verification, and business licensing system and • External Point of Sale system(s). 	YES	106
3.4x	Unique Identification Tag/Labels	<p>The system must utilize a readable smart-chip technology including Radio Frequency Identification or RFID, or comparable technology to track cannabis plants and product. The smart chip technology should contain the following information:</p> <ul style="list-style-type: none"> • Plant tag unique identification number • Plant grow address • Plant Owner License Identification Number • Tag issue date • Any other information required by the State unique identification number • Plant grow address • Plant Owner License Identification Number • Tag issue date • Any other information required by the State 	YES	108
3.4y	Unique ID Printer/Plant ID Printer	<p>The proposed solution must offer a unique identification code printing capability to streamline the inventory and chain of custody record keeping for Cannabis Establishment Employees and the State personnel.</p>	YES	110



Security & Maintenance (proposal section IV.b.4)				
3.4z	Plant ID Reader	The proposed solution must offer a barcode scanning capability for unique identification to be used by Cannabis Establishment Employees and the State personnel.	YES	110

Operation (proposal section IV.b.5)				
ID	CATEGORY	REQUIREMENT	YES/NO	PAGE REF. IN PROPOSAL
3.5a	Previous Government Experience	The vendor must provide a minimum of 2 example of a successful software implementation of a system similar to this RFP and 3 references from governmental agencies.	YES	112
3.5b	Legislative Updates	The vendor must provide legislative and regulatory updates within the scope of the proposed 5-year bid/contract at no expense to the State	YES	117
3.5c	Risk Management and Communication Plan	The vendor must provide a written risk management and communication plan for the proposed 5-year term of the contract.	YES	118
3.5d	Training Plan	<p>The vendor must provide a training plan for both internal and external users. Training plan should include the following items and estimated completion: timeframe for each of the item:</p> <ul style="list-style-type: none"> • Training Needs Analysis: topics should include but not limited to the following: <ol style="list-style-type: none"> 1. System configuration 2. User Administration 3. Security Features 4. Password Reset Instruction 5. Functionality related to the inventory and chain of custody management for the manufacturer, transportation, testing, distribution, recall tracking, sale, and reporting. 6. Reporting Features 7. For technical staff, the use of the platform API • Role Based Training Materials • Webinar Based Training • End User Manual and Material Updates: • Periodic Training Assessment Review 	YES	121



IV. Detailed Response

This section should constitute the major portion of the proposal and must contain at least the following information:

- a. A complete narrative of the offeror's assessment of the work to be performed, the offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the offeror's understanding of the desired overall performance expectations.*
- b. A specific point-by-point response, in the order listed to each requirement in the RFP. The response should identify each requirement being addressed as enumerated in the RFP.*
- c. A clear description of any options or alternatives proposed.*

Metrc's approach to traceability is to establish the most robust and reliable regulatory dataset available: a single, centralized database of every single legal marijuana plant and product in the supply chain. Such a database provides regulators with near real-time insight into aggregate market performance alongside granular product information, such as where each product is located, where it came from, how it tested, who touched it, and where it ultimately sold.

While our system is designed for regulators, it is ultimately dependent on licensees and the accuracy of the data they report. To fill this database, every licensee in the supply chain enters information into Metrc's database each time they interact with their plants or products, creating a single source of truth for regulators.

The following is an assessment of the work to be performed, a point-by-point response to the requirements, and proposed options.

IV.a. Narrative of Metrc's Assessment of Work to be Performed

The following narrative of Metrc's assessment of work to be performed includes the following topics:

- Approach and Methodology, p. 22
- Resources to Fulfill Requirements, p. 30
- Record of Past Performance, p. 35
- Availability and Familiarity with Project Local, p. 37
- Project Management Techniques, p. 37
- Ability and Proven History Handling Special Project Constraints, p. 41



IV.a.1. Approach and Methodology to Meet Project Requirements

To describe Metrc's approach and methodology to meet project requirements we address each of the State's seven deliverables on the following pages: 1) Kick-off, 2) Project Plan, 3) Gap Analysis, 4) System Configuration, 5) Acceptance Testing, 6) Training, and 7) Implementation.

IV.a.1.(1) Kick-off

Participate in a kickoff meeting to discuss these features and produce a project plan. Kickoff meeting must facilitate the introduction of the State and the Vendor core project members, and level set understanding of project objectives, timeline, scope, and project risk and issues.

The State's project begins with a project planning and kick-off meeting, with core project members from the State and Metrc teams, to define and create consensus on project details such as project objectives, timeline, scope, project risk and issues, high-level requirements, milestones, and resources. The teams also work to define administrative procedures, project management guidelines, and communication protocols. The kick-off meeting includes key staff from the State and senior leadership, engineers, and project managers from Metrc.

IV.a.1.(2) Project Plan

The Vendor shall collaborate with the State to develop a baseline project plan which includes project schedule.

Metrc will collaborate with the State to develop a project plan that includes a project schedule. During the planning phase and concurrent with the discovery activities, Metrc begins turning the proposed high-level project plan into the detailed project plan and schedule for the project. Discovery activities inform the detailed activities, tasks, and resources required for a successful implementation. The State's project manager reviews (or is walked through) the draft plan, and we incorporate input before baselining the plan.

Metrc follows a robust and field-tested project plan that we have honed over the past decade across 16 implementations. While every implementation is different, they nonetheless entail similar key activities and milestones. This allows for Metrc's project plan to be quickly and easily tailored to the State's unique needs and timeline.

We have included an overview of our implementation process and a sample project schedule based on a six-month implementation timeline below in response to 3.4u on page 96.



IV.a.1.(3) Gap Analysis

The Vendor must review, analyze, and confirm the understanding of system functionality, business practices, interfaces, configuration and customization. The analysis should include the demonstration of how the system meets the requirements as defined in the Section 3 of this RFP, and any required configurations to meet the requirements.

Metrc conducts a fit/gap analysis during Phase 1 of the project implementation process—the fit/gap analysis is our primary process for tracking implementation success and reviewing, analyzing, and confirming our understanding of system functionality, business practices, interfaces, configuration, and customization.

The fit/gap process involves evaluating every requirement (as defined in the Section 3 of the State's RFP) against current functionality to validate as a "fit" (functionality meets requirement) or identify a "gap" (additional development is required for functionality to meet requirement). The analysis is reviewed with State stakeholders and becomes the foundation for project development work and implementation.

The fit/gap analysis also provides us an opportunity to identify areas that may not have been addressed in the original requirements. Since the regulated cannabis marketplace is effectively new for most regulators, there are typically items identified through our analysis that have led to new requirements. For example, during our fit/gap analysis with the State of Ohio, they discovered a need to identify unique item types more granularly than our standard item categories. Metrc developed unique item identifiers for them that met those specialized needs for the first time in the United States.

After the fit/gap analysis, we perform extensive quality assurance (QA) reviews to ensure that the functionality is configured or customized, as appropriate, and that it operates correctly and fulfills the core requirements. Information from the QA reviews is then catalogued in our requirements tracker.

IV.a.1.(4) System Configuration

The Vendor shall configure the system according to the requirements established during the gap analysis and RFP.

Metrc will configure the Metrc System according to the requirements established during the fit/gap analysis (and other Phase 1 planning processes) and within the RFP. The System was built specifically to help regulators track and trace cannabis products from seed to sale. As such, it is highly adaptive and enables changes to be made quickly and easily as laws and regulations evolve over time. Fortunately, over 90% of client agency requirements are typically met by configuration of the current System, meaning that less than 10% of requirements require custom development work. This results in a streamlined and straightforward implementation process.



When enhancements are needed, we can develop them quickly because the System is highly configurable. While some of the System's core functionality is periodically updated for all users (e.g., with security and performance enhancements), every client agency, including the State, receives an individualized and separate instance of the System. These instances are specifically configured to each agency's unique needs. As Metrc makes System enhancements in response to requests from other agencies, we make them available across all System instances. Any agency may opt out, but the approach provides the option for agencies to benefit from the experience and improvements made by other agencies.

Configuring the Metrc System

We identify configuration requirements through several methods, including:

- Statutory and regulatory review
- Fit/gap analysis
- User acceptance testing
- User training

While executing the above processes, we use a testing environment that includes all available features and configurable items in the Metrc System. We then work with the State in the testing environment to identify the baseline functionality and items that require configuration. Following this, we begin the change control process to document, develop, and review system updates with the State.

We record and report on the status of changes throughout the development process in the following deliverable documents:

- Preliminary fit/gap analysis
- Business requirements review
- Requirements validation report
- Project Implementation plans

These actions allow the State to regularly audit the configuration, ensuring that all changes meet the State's specific requirements and shifting needs. They also allow Metrc and the State to control:

- Build management: Managing the process and tools used for builds.
- Process management: Ensuring adherence to the organization's development process.
- Environment management: Managing the software and hardware that host the System.
- Defect tracking: Ensuring that every defect and corresponding resolution has traceability back to its source.

Our process allows the State to have complete control of configuration management for evaluating, coordinating, approving, and implementing changes specific to its instance of the Metrc System.



State-Configurable Items

The System has numerous elements that can be configured directly by the State's administrator (or with assistance from the Metrc team).

State-configurable areas include:

License Types: The State can create license types. It can also set different tiers for each license type, e.g., Cultivation Tier-1, Cultivation Tier-2. These updates are often used to align with the State's unique licensing rules and system (e.g., different tiers for different sizes of licensees).

Employee Types: The State can create specific user profiles for licensee users and licensees with corresponding permissions. For example, common industry user types include Administrator, Manager, and other industry occupational roles. These employee types will have specific permissions on what data and functionality they can access.

Item Categories: The State can create item categories that are specific to that jurisdiction's various cannabis products. "Item category" is synonymous with "product type" and enables both industry and the State to categorize thousands of products into common, discrete categories. For example, an "infused non-edible" category type would include all tinctures, topicals, suppositories, and oils. While we have many commonly used categories that we can recommend, each agency is able to create as many item categories as desired.

Action Reasons: The State can create action reasons that enable licensee users to notate why specific actions or events occurred. For example, a licensee user may need to adjust a package inventory because of spoilage, waste, or input error or may reject a transfer because it arrived after hours, included an incorrect package, or was the incorrect weight. Similar to item categories, action reasons enable the users to provide common, discrete reasons for specific actions they may be taking and enabling simpler reporting.

Administrative Hold Reasons: The State can create the reasons behind placing a specific product on hold. (When products are placed on hold, they cannot be placed on a manifest, shipped, or transferred by a licensee. Held products are highlighted in red in the System, and licensees see a notification banner in the System upon login.) These hold reasons indicate to the industry why, pursuant to regulation, their products are being placed on administrative hold. They may include specific violations of rules or testing procedure.

Transfer Types Limits: The State may set transfer types, which include the ability to set limitations for certain products. Licensees will not be able to arrange a transfer in the System of any product that exceeds these limits.

Lab Tests Types: The State can create the various lab test types that its licensed products must undergo. Common test types include potency, pesticides, micro biologicals, and homogeneity. Test types are specific to the client agency's local regulations around testing.

Remediation Methods Process: In the case of testing failures, the State can specify if and how product can be remediated, the requirements for doing so, and the notifications and identifiers.



For example, if licensee's product failed for water activity (meaning the flower was too wet), the licensee could remediate by allowing the flower to dry longer and retest. If it failed for mold on flower or trim, the licensee could remediate by extraction process.

Tax Rates: The State can control product tax rates and percentages from the Administrator view. The System can be enhanced to calculate taxes throughout the jurisdiction on any transaction processed in the System (including through point-of-sale integrators).

Rules Engine: The System's rules engine allows the State to configure customized notifications of events to specific users, user types, and/or organizations. Virtually any event in the System can create a notification, such as selling after hours, selling over the limit, and transferring over the limit. The rules engine can create hundreds of types of notifications from any aspect of reportable information from any licensee in the System.

State-configurable items are designed to give the State the freedom and flexibility to implement commonly used and easy-to-implement configurations, without going through an extensive and costly change management process with Metrc.

IV.a.1.(5) Acceptance Testing

The Vendor shall develop a testing management plan that outlines the overall testing approach and schedule. Additionally, the Vendor must support the State's testing efforts, make changes, and remediate testing issues during the State's user testing period.

Metrc's testing management plan will outline our overall testing approach and schedule. Metrc's System Test Plan defines the structure used to test each specific software product to ensure it meets the requirements that guided its design, is sufficiently usable, and can be installed and run in the intended environments. It includes plans for various tests including the unit test plan, system-specific user acceptance test plan, and security test plan. Metrc's test lead designs a suite of automated user acceptance tests of the System's functionality. The functionality is tested with circumstances expected to pass and circumstances expected to fail.

Unit Test Plan: Metrc's Unit Test Plan sets out the procedure by which we test the individual units of source code and/or program modules with associated control data.

User Acceptance Test (UAT) Plan: The UAT Plan defines the procedures by which we test the user acceptance criteria, the load capability, and any regression testing required. Metrc business analysts perform the UAT, load capability testing, and any regression testing. They also write and perform the prescribed testing. The System generates a report detailing the list of tests performed and their pass/fail status. We will also support the State in conducting its UAT efforts and make changes and remediate testing issues during the State's testing period.

Security Test Plan: The Security Test Plan defines the test methods we employ to ensure that the System is secure. We perform security testing by using the Veracode Static Analysis platform to verify that the System protects data and maintains functionality as intended. We test the System to ensure that confidentiality, availability, authorization, integrity,



authentication, and non-repudiation are maintained. Our developers use the Veracode Static Analysis platform testing to generate results that are prioritized based on severity for remediation. Our developers also use Veracode's Web Application Security platform to test the System for architectural weaknesses and vulnerabilities in running web applications, then provides validation or items for remediation.

For additional details about our testing program, please see 3.4u on page 94.

IV.a.1.(6) Training

The Vendor must create a training management plan that includes training approaches, courses, schedules, and required resources. Additionally, the Vendor must conduct the end user and administrator system training and provide up-to-date user manuals by end user types.

We have provided comprehensive details about our Training Plan and Program (including training materials provided) below in response to 3.5d, on page 121. The following provides an overview of our approach.

Training Management Plan

We develop a Training Plan as part of the project management process. It will include training approaches, courses, required resources, and a proposed training schedule, which we will fine-tune collaboratively during the project kick-off meeting.

Metrc's support and training teams' driving goal is to ensure State staff and licensees can use the System effectively and with ease. This starts with a highly qualified support and training staff, extends to a comprehensive training program, and continues with ongoing, unlimited support.

Metrc training team members are all full-time, U.S.-based Metrc employees. We do not outsource our training. Metrc's user training program is designed to ensure that State and licensee users can work proficiently on the Metrc System. User training is unlimited and offered at no additional cost to users or the State.

We customize trainings to meet each client's specific needs. Trainings can also accommodate users from other agencies, such as Investigators, Information Technology (IT), and others. This approach ensures that all stakeholders can effectively leverage the System if desired by the State.

A successful track-and-trace program depends on licensees being able to use the System effectively. To support that need, Metrc provides a dedicated training staff and comprehensive training program for licensee users. At the start of the training program, Metrc training team members collaborate with the State to understand the various groups who will need trainings (e.g., owners/administrators, staff, third-party integrators, etc.). They then develop and customize training content for each.



IV.a.1.(7) Implementation

The Vendor shall collaborate with the State to create an implementation plan that includes strategy, tasks, go/no-go decision requirements, and implementation contingency plan. For implementation, the Vendor is responsible for providing technical support and make fixes required in a timely manner to implement the system in accordance to the agreed upon schedule.

Implementation Plan

Per the State's requirements, Metrc will provide an expedited six-month implementation. Metrc's Implementation Plan is a comprehensive plan that includes details about the following: the Metrc System, implementation process (strategy, tasks, go/no-go decision requirements), fit/gap analysis, communication, time management, scope management, issue management, risk management, system configuration, State administrator configurable items, quality assurance, metrics, testing, third-party vendor integration, and an implementation contingency plan.

The following provides an overview of Metrc's five-phase implementation process as demonstrated below in Figure 1. Operating concurrently with all five phases are ongoing activities that support on-time delivery and continuous improvement.

These include:

- Weekly status reports
- Ongoing documentation updates
- Requirements tracking and validation
- Future-state feature planning
- Stakeholder engagement, approval, and escalation
- User training and support

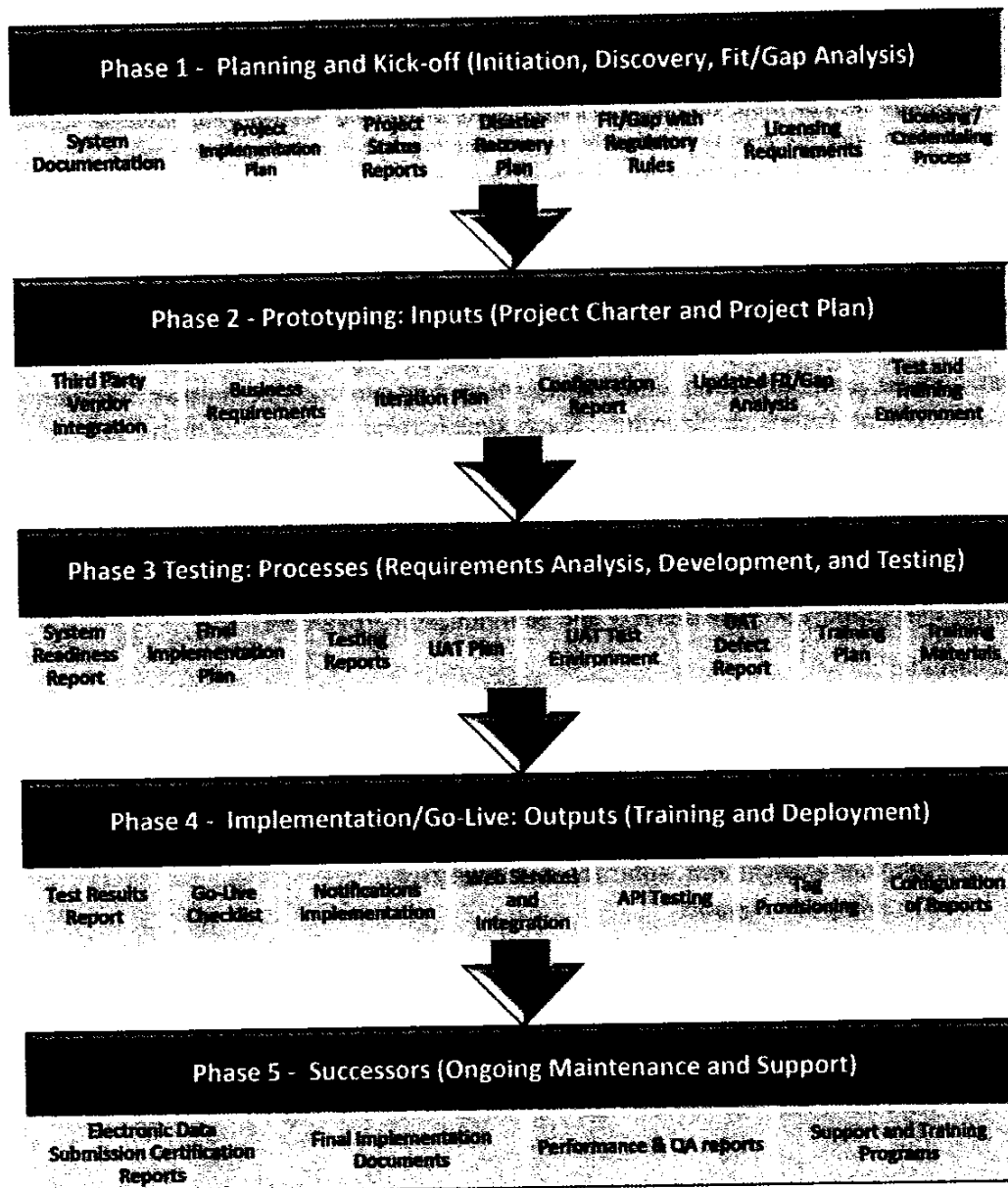


Figure 1. Proven Project Implementation. *The State's project will follow a structured Project Management Body of Knowledge (PMBOK)-based waterfall approach to ensure your System is delivered on time, within budget, and meets all project requirements and expectations.*

Technical Support and Fixes

Throughout the implementation, and for the duration of the contract, Metrc will provide technical support and make required fixes in a timely manner to both implement the System in accordance with the agreed upon schedule and provide ongoing system management and enhancements, as required. Highlights of the support the State can expect include:



- 24/7 access to support team management at no additional cost—direct access to an assigned contract manager and our senior leadership.
- A Systems Issues Team dedicated to handling System issues and ensuring that all reported issues follow the requirements outlined in the Expected Process for Incident Reporting and Severity Table (see page 100).
- A Level Three Support team consisting of people from our engineering, development, and business management teams. They provide State users with quick resolution, feedback, troubleshooting, and support for complex issues. (See 3.4t for details.)
- A team of full-time technical and engineering staff at our Lakeland, Florida offices. At any time during non-office hours, at least one technical and engineering team member is on call.

For details about each bullet listed above, as well as a detailed description of our Support Program, please see our response below to 3.4.t, on page 90.

IV.a.2. Resources to Fulfill Requirements

Metrc's executive and implementation teams are comprised of industry-leading experts with more than nine decades of combined experience in the regulatory, cannabis, and technology fields. We are passionate about how the Metrc System supports regulatory efforts to protect public health and safety and will work scrupulously with your team to ensure that it is effectively configured and delivered.

Metrc's executive and implementation leadership teams will be intimately involved in the State's implementation. They will oversee the implementation leads and ensure that all contract activities are met.

The Program Management team, comprised by David Eagleson, Nick Figueroa, and Riley Sisk, will lead the on-the-ground support and training efforts for your project. They are also responsible for committing the resources necessary to properly staff implementation, maintenance, and support for the duration of your contract. David will provide oversight, Nick will be the engagement lead and the State's primary point of contact from Metrc, and Riley will provide additional project support during implementation.

Along with the Program Management team members, seasoned professionals from several of our other teams will support the system implementation and its ongoing management, including attending the project kick-off meeting, onsite meetings, roadshows, and trainings.

Below is a RACI (Responsible, Accountable, Consulted, Informed) chart that illustrates how our team will work together to implement and support the State during this project. "Responsible" is the individual responsible for carrying out the process and getting the job completed; "Accountable" is the individual ultimately accountable for the task's completion; "Consulted" are the individuals who are consulted but not directly involved with carrying out the task;



"Informed" are the individuals who receive outputs and/or need to stay informed on progress.
Bios for the key individuals in the RACI chart follow.

PHASE	FUNCTION/ COMPONENT	RESPONSIBLE (R)	ACCOUNTABLE (A)	CONSULTED (C)	INFORMED (I)
ALL PHASES 1-6	Project Oversight	Lewis Koski	Jeff Wells		
1. PROJECT IMPLEMENTATION PLAN AND STATUS REPORTS	Implementation Planning and Schedule Development	David Eagleson Nick Figueroa Riley Sisk	Lewis Koski	Cherie Denholm Jennifer Clements	Jesse Naranjo
2. BUSINESS NEEDS ANALYSIS	Requirements Gathering and Analysis	David Eagleson	Lewis Koski	Cherie Denholm Nick Figueroa Jennifer Clements	Jesse Naranjo
	Design Documentation	Jennifer Clements	Jesse Naranjo	David Eagleson Nick Figueroa	Lewis Koski
	Installation, Configuration, & Hosting	Jennifer Clements	Jesse Naranjo	David Eagleson Nick Figueroa Cherie Denholm John Stephens	Lewis Koski
	Security & Performance Calibration	Joey Perdomo	Jesse Naranjo	David Eagleson Jennifer Clements Nick Figueroa	Lewis Koski Cherie Denholm
3. SOFTWARE CONFIGURATION	Fit/Gap Analysis	David Eagleson	Lewis Koski	Cherie Denholm Nick Figueroa Jennifer Clements	Jesse Naranjo
	Configuration Development & Management	Jennifer Clements	Jesse Naranjo	David Eagleson Nick Figueroa	Lewis Koski Cherie Denholm
4. SYSTEM TESTING	Testing Development & Reporting	Jennifer Clements	Jesse Naranjo	David Eagleson Nick Figueroa	Lewis Koski Cherie Denholm
	Business Continuity	David Eagleson	Lewis Koski	Cherie Denholm	Lewis Koski



PHASE	FUNCTION/ COMPONENT	RESPONSIBLE (R)	ACCOUNTABLE (A)	CONSULTED (C)	INFORMED (I)
	Planning & Reporting			Nick Figueroa Jennifer Clements	Jesse Naranjo
5. SYSTEM IMPLEMENTATION	User Acceptance Testing & Quality Assurance	David Eagleson	Lewis Koski	Cherie Denholm Nick Figueroa Jennifer Clements	Jesse Naranjo
	User Training	Cherie Denholm	Lewis Koski	Nick Figueroa David Eagleson Jennifer Clements Rob Romig	Jesse Naranjo
	Go-Live & Readout	David Eagleson	Lewis Koski	Cherie Denholm Nick Figueroa Jennifer Clements	Jesse Naranjo
6. ONGOING DELIVERY OF SERVICES	User Support & Training	Cherie Denholm	Lewis Koski	Nick Figueroa David Eagleson Jennifer Clements Myra Chin Tricia Mills Rob Romig	Jesse Naranjo
	Maintenance, Ongoing Enhancements, & System Security	Jennifer Clements	Jesse Naranjo	David Eagleson Joey Perdomo Nick Figueroa	Lewis Koski Cherie Denholm
	Monitoring & Reporting	Nick Figueroa	David Eagleson	Lewis Koski Jennifer Clements Cherie Denholm	Jesse Naranjo



Key Staff Bios

Jeff Wells, Chief Executive Officer

Jeff is the Chief Executive Officer (CEO) of Metrc and one of the co-founders of its predecessor Franwell. Jeff has been involved in every implementation across 15 states and the District of Columbia. Jeff has over 30 years of experience in software development and over 15 years of experience in research, development, and implementation of RFID and supply chain technologies.

Lewis Koski, Chief Operating Officer – Executive Sponsor

Lewis Koski is Metrc's Chief Operating Officer. Before joining Metrc in 2019, Lewis ran his own consulting firm where he helped government agencies develop cannabis policies. Prior to that, he served as the director of the Colorado Marijuana Enforcement Division and helped build the first U.S. state agency to develop and implement medical and adult-use cannabis regulations. Lewis holds a doctoral degree in public policy from Walden University and serves on the advisory board of The Policy Center for Public Health and Safety (PH&S). Lewis will be Metrc's executive sponsor of the State's implementation and its main executive contact.

Jesse Naranjo, Chief Product Officer – Executive Sponsor

Jesse Naranjo is the Chief Product Officer for Metrc. He has been with the company and its predecessor Franwell for nine years and has direct hands-on experience with building out every facet of the Metrc track-and-trace system. He has more than 14 years of combined experience in software administration, development, and support. Before being named Chief Product Officer, Jesse served as Chief Technology Officer, and was also the company's lead software developer. In his current role, Jesse will be in charge of product development and will facilitate the design and implementation of Metrc's core system deliverables from conception through the implementation of a go-to-market strategy.

David Eagleson, Director of Program Management – Project Engagement Manager

David Eagleson was hired as a Program Manager for Metrc in 2017, leading state implementations and managing the company's ongoing relationships with Massachusetts, Michigan, Ohio, and the District of Columbia. He currently leads Metrc's national office of Program Management and works in close association with a staff of eight dedicated program managers.

David's Program Management team maintains close working ties with government agencies on a range of regulatory business, including rules and regulations review, project planning, system configuration analysis, fit/gap analysis, user acceptance testing, state and industry presentations, among other action items. David, together with the Program Manager he oversees, will be the main points of contact for the State. They will lead the project kickoff meeting in partnership with the State, ensuring all other activities are met, while helping to facilitate the State's requests on an ongoing basis.



Nick Figueroa, Lead Program Manager - Implementation Lead & Ongoing Project Manager

Nick Figueroa is a government Program Manager for Metrc. He has been with the company since 2019 and has managed efforts in numerous statewide activations, including those in Ohio, Maryland, and the District of Columbia. Nick has also played a pivotal supporting role for company efforts in West Virginia and Maine. As the principal day-to-day project contact for state agencies and representatives, he manages multiple requirements around rule and regulation reviews, contract amendments, project planning, industry outreach, system configuration analysis, API integration, and related aspects of client service and management.

Prior to joining Metrc, Nick was a Senior Customer Success Manager at Resilinc Corporation, based in Milpitas, California. In addition to being the principal liaison for product management, data operations, and the engineering arms of the company, he was charged with helping new customers master Resilinc products and updated software modules. He also consulted with Fortune 500 companies to assist them in building resilient supply chains. These efforts included crisis management and response, business continuity planning, corporate social responsibility, and conflict mitigation. Nick will be the State's point person, providing day-to-day point-person contact with State project staff to ensure the smooth implementation of Metrc's track-and-trace solution, while ensuring that Metrc is meeting all agency directives, guidelines, and expectations.

Riley Sisk, Program Manager – Implementation & Project Management Support

Riley Sisk is a government Program Manager for Metrc. He has been with the company since 2019 and has managed numerous statewide activations, including those in Oregon, Missouri, and Michigan—now the fourth largest cannabis market in the country. As the principal day-to-day project contact for those state agencies and representatives, he manages multiple requirements around rule and regulation reviews, software updates, contract amendments, project planning, industry outreach, system configuration and analysis, API integration, and related aspects of client service, communications, and management.

Prior to joining Metrc, Riley served as a professional services consultant in implementation for Epicor Software, based in Minneapolis. In addition to providing guidance on software functionality and supply-chain operations, he coordinated company-wide projects across all levels of the organization. Prior to that, he served as an international customer logistics liaison for Land O' Lakes, where he managed multiple Enterprise Resource Planning (ERP) projects, including system design, IT, and business team coordination. Riley will support Nick to ensure the smooth implementation of Metrc's track-and-trace solution.

Jennifer Clements, Product Owner – Configuration Lead

Jennifer Clements is Metrc's Product Owner, reporting directly to the CPO. In her current role, she helps guide and motivate members of her team to meet State objectives, including all project deliverables. Jennifer is also involved in maintaining key timelines and reporting out progress on schedule compliance, engineering standards, and any necessary procedures that are critical to the project's success.



Jennifer has been with Metrc since 2016. She has served as engineering quality assurance analyst and later served as an engineering project manager, where she worked closely with state agencies and representatives to coordinate the on-time delivery of all client-facing products. Jennifer has been heavily involved in nine state implementations and maintains an ongoing technical relationship with Metrc's client agencies. She is most involved in systems analysis, development, and testing; state implementations and set ups; and ongoing maintenance and support activities.

Cherie Denholm, Director of Support and Training – Support & Training Lead

Cherie Denholm is Metrc's director of support and training, reporting directly to the COO. She has nine years of experience at Metrc and has been deeply involved in every one of the 16 implementations that the company has undertaken to date. In her current role, Cherie leads over 70 professionals in support, training, and enforcement.

In addition to determining client proficiency with Metrc systems, Cherie was instrumental in the creation and oversight of the User Acceptance Testing (UATs) program, critical to Metrc's success. The State and licensees will have access to the full suite of support and training resources Cherie leads. She will be closely involved in the implementation and set up phase, will lead state and licensed entities training programs, and supervise ongoing maintenance and support activities.

Metrc has provided key staff resumes in **Attachment 1**.

IV.a.3. Record of Past Performance

Metrc has proven past performance and experience to provide the system and services the State seeks. Metrc is the leading provider of track-and-trace solutions, with 10 years of experience partnering with public-sector clients overseeing cannabis markets. The following details attest to our record of exceptional performance:

- The State of Colorado partnered with Metrc in 2011 to develop the first statewide track-and-trace system for marijuana; since then, 15 other jurisdictions have partnered with us.
- In the jurisdictions we serve, Metrc has over 1,400 regulatory users and 240,000 licensee users from over 30,000 licensed businesses.
- Our regulatory clients have used the Metrc System to track almost \$24 billion in sales and over 1 billion supply chain events, such as plantings, harvests, packages, transports, and tests.
- Metrc has more track-and-trace contracts (for medical and adult-use markets) with government agencies than any other vendor, and we are the only vendor with a 100% renewal rate on those contracts. Founded in 1993 in Lakeland, Florida, our original parent company, Franwell, Inc. (Franwell) provided supply chain solutions for highly regulated products like pharmaceuticals and food. In 2010, Franwell expanded its



capabilities to the cannabis industry by designing the first track-and-trace system in close collaboration with state regulators in Colorado. In 2012, the system went live and, following Colorado's success, other states like Oregon, Alaska, and Maryland saw the value in track-and-trace systems and partnered with Franwell to implement them.

In 2017, Franwell formed Metrc LLC (Metrc) to focus exclusively on cannabis. And to continue growing the team, we received a \$50-million investment from two venture capital firms. Their investment demonstrated a major vote of confidence in our business model, our product, and—most importantly—our people. Metrc's solution is reflective of our decades of experience in tracking and tracing regulated inventories, and we are confident that the Metrc System is the best, most robust, and most secure product on the market.

In August 2019, the Colorado Office of the State Auditor called Metrc the "cornerstone of the state's regulatory structure for medical and retail marijuana," and multiple states used the System to identify and prevent potentially harmful vaping products from being sold during the nationwide vaping emergency in the U.S. Metrc has now grown to over 130 employees and, in addition to Colorado, partners with regulatory agencies in 15 other U.S. jurisdictions for their cannabis track-and-trace systems: Alaska, California, Louisiana, Maine, Maryland, Massachusetts, Michigan, Missouri, Montana, Oklahoma, Nevada, Ohio, Oregon, West Virginia, and the District of Columbia. Eight of the jurisdictions use the System to monitor their medical marijuana markets, and the other eight use it to monitor both their medical and adult-use markets.

Metrc delivered our solution for each of our clients on time, and within budget—we do whatever it takes to ensure full client satisfaction with our software and services. Our cost control is rooted in our philosophy to be highly flexible and include all reasonable enhancements at no additional cost to the State, given how rapidly cannabis policy can change. In rare circumstances, our client agencies have requested features that were mutually determined to be out of scope, such as the creation of a public-facing product catalog in Massachusetts. In those rare instances, we collaborated with our clients to determine the best and most cost-effective way to achieve their requirements, agreed on a budget and timeline, and only began work after their clear signoff.

Metrc's executive and implementation teams represent over nine decades of combined experience by industry-leading experts from the regulatory, cannabis, and technology fields. Collectively, we are passionate about how the Metrc System supports regulatory efforts to ensure public health and safety. Our partnership with the State will combine your knowledge and insights with our extensive expertise to ensure that the Metrc System is successfully configured and delivered from implementation and throughout the lifetime of our contract.

We have provided references (per RFP section 4.4) in response to requirement 3.5a on page 121, as well as written letters of recommendation in **Attachment 2**. Summary pricing is also included in that section for five of our contracts, and if the State desires additional detail, Metrc will provide copies of any of our state contracts, including pricing, upon request. We encourage



the State to contact each of the points of contact listed to validate Metrc's past performance and our client satisfaction.

IV.a.4. Availability and Familiarity with Project Locale

Metrc is fully willing and able to have staff available on site as needed in Pierre, South Dakota. All implementation staff are based in the continental United States and are full-time employees of Metrc.

While Metrc is headquartered in Lakeland, Florida, we follow a remote-work model, where the majority of our employees are based remotely. This means that our employees are highly experienced and proficient leading virtual meetings and are well acquainted with work travel for both client and internal needs.

Metrc has used our remote-work model in each of our previously mentioned 16 implementations and achieved an excellent record of quality, customer satisfaction, as well as schedule and cost maintenance in each one. Along with the Program Management team members, seasoned professionals from several of our other teams will attend onsite meetings in South Dakota, including for kickoff, roadshows (educational sessions), initial trainings for State and licensee users, and any other high-priority or ad-hoc meetings, as requested by the State. Metrc proposes hosting the kickoff in Pierre at State facilities, and the roadshows for licensee users would take place in Sioux Falls and Rapid City, with the potential to expand to other regions of the state (e.g., northeast and northwest), as informed by licensee presence and interest.

As part of our proven implementation and ongoing management model, Metrc makes key personnel available for in-person meetings and incurs the cost of travel, meaning no travel-related expenses will be charged to the State under this contract. We look forward to demonstrating this proven approach with the State.

IV.a.5. Project Management Techniques

Metrc uses a hybrid Agile/Waterfall project management approach that has been proven over time with our current clients. We leverage the Agile methodology in software customization, development, configuration, and deployment activities for all Metrc System implementations. The Agile approach uses "sprints": short, time-boxed iterations of work meant to break down big, complex projects into smaller, more manageable tasks – allowing for more frequent reviews and improvements. Then we use a more traditional, structured PMBOK-based Waterfall approach with project implementation and reporting. This blending of methodologies allows our project to be nimble and responsive to change while ensuring quality work products, comprehensive system documentation, and full traceability of customization and configuration activities are always available to the State. Our approach for the State's project will ensure that



your Metrc System is delivered on time, within budget, and meets all project requirements, objectives, and expectations.

Metrc will assign an experienced project manager (PM) to your project. The PM will be responsible for all tasks necessary to manage, oversee, and ensure the project's success, including developing and updating project plans, assigning staff members, scheduling meetings, circulating status reports, addressing project concerns, and more.

"We appreciate Metrc's ability to deliver a completed track-and-trace solution within one of the tightest timeframes imaginable. Thanks to the dedication and hard work of the Office of Marijuana Policy and Metrc teams, this important milestone was realized—as scheduled—at the end of March [July 2020]. We look forward to a long, productive relationship and utilizing Metrc to help ensure the success of the programs we regulate."

- Erik Gunderson, Director, Maine's Office of Marijuana Policy

Time Management

Metrc uses time management to prioritize product delivery and manage scope. As requirements and dependencies are defined, the development team estimates the hours required to fulfill them. All tasks designed to be completed in 8- to 80-hour increments. The development and program management teams then develop a delivery schedule based on these estimates, resources assigned, and priority.

Scope Management

Metrc's established scope management process ensures that development work proceeds on schedule, aligns with your needs and expectations, and remains focused on agreed-upon, priority deliverables.

The scope management process follows these general steps:

- Define requirements and perform fit/gap analysis.
- Determine priorities and required levels of effort.
- Assign and document sprints to satisfy specific requirements. (Each sprint is a work cycle that generally lasts 30 days and is designed to meet specific requirements.)
- Obtain sign off from stakeholders on sprint goals.
- At the end of each sprint, compare completed functionality to the original requirements to determine if further development work is required.



This approach ensures that development work is always tied to predefined and agreed-upon requirements. It keeps all teams focused and minimizes scope creep (expansion of project scope with non-priority requirements/needs). And, while our process does allow for requirements to be added over time, they must go through the initial definition and prioritization process and be signed off on by all stakeholders before being incorporated into the scope.

We also manage scope using an automated deployment and release management tool. The tool works with Metrc's build server to enable reliable, secure, automated releases of ASP.NET applications and Windows Services into test, staging, and production environments.

Project Management Tools

Collaboration is critical with projects like yours. Given that, we use a secure, collaborative online project management tool called Teamwork that project team members can access throughout the implementation and system development process.

Teamwork gives project team members anywhere, anytime access to the detailed project schedule and other project components. It helps streamline communications and processes, including communication around responsibilities, commitments, activities, and deadlines (see Figure 2). It helps team members track tasks and serves as a document repository for project artifacts, allowing team members to easily find plans, documents, and other important items quickly and easily.

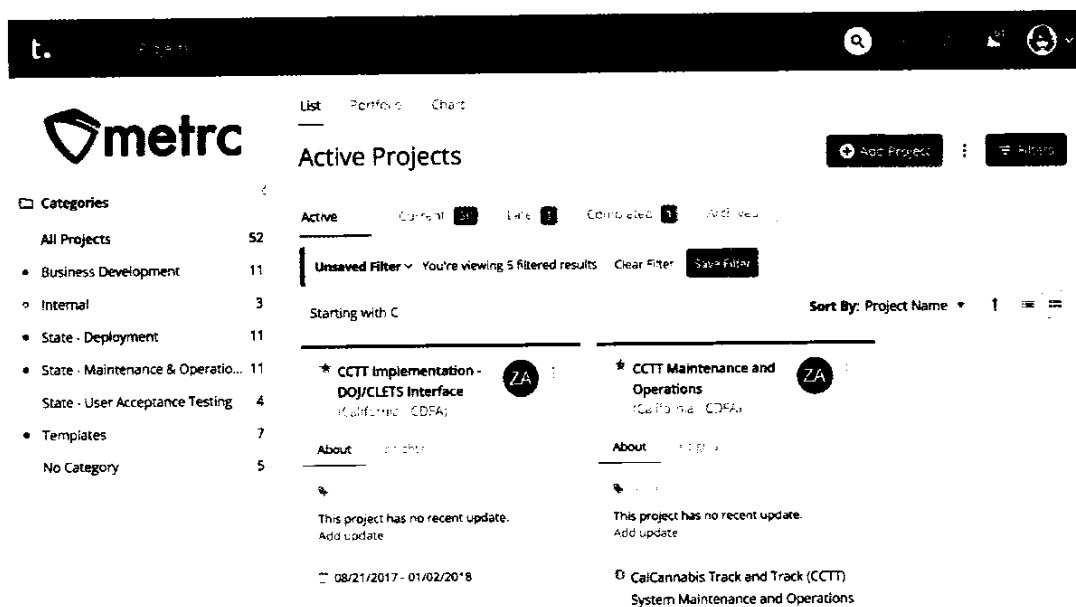


Figure 2. Anytime Access. Teamwork ensures consistent and efficient collaboration and delivery.



Teamwork is task driven and provides our team with the following project management tools:

Teamwork's Project Management Tools	
Customizable tasks, subtasks, and dependencies	Roles and associated permissions
Customizable milestones	Risk logs
Activity reports	Date and time reporting
Program file and document storage	Automated e-mail alerts
Management activity dashboard	Document editor with previews
Notebooks	Reminders
Messages	Tags and notifications
Gantt charts	Project trends

Metrc will grant access to State staff to view and collaborate on tasks in Teamwork. Tasks can also be exported as a PDF or Excel spreadsheet for offline review and reporting.

Additionally, Metrc can deploy DocuSign for the facilitation of signatures for key deliverables, if desired. DocuSign allows for signatures to be gathered sequentially by the necessary team members and sends reminders when a document is pending review. It helps speed up document review and approvals over the span of a project.

Communication Resources

Metrc's communication and resource management approach includes a Communication Management Plan and Teamwork, our collaborative project management tool. The Communication Management Plan establishes how communications with project team members, project stakeholders, senior staff, and the public (if appropriate) will be handled throughout the project lifecycle. We provide details about our approach in response to 3.5c on page 118.

Risk and Issue Management

Metrc's Risk Management process follows the guidance provided by the National Institute of Standards and Technology (NIST) "Guide for Conducting Risk Assessments" to monitor, manage, and mitigate risk. We provide details about our approach to risk and issue management in response to 3.5c on page 118.



IV.a.6. Ability and Proven History in Handling Special Project Constraints

Metrc does whatever it takes to meet our contractual obligations and exceed our client expectations. This often means that we are tasked with accommodating special project requests given policy, legal, or other constraints. The following describe a number of examples of such constraints, such as the rapid expansion of our solution to a newly legalized adult-use market, and how we addressed them.

Co-Located Inventory Management: In jurisdictions that allow for both medical and adult-use facilities to be co-located, there have been challenges enabling licensees to easily identify and manage separate inventories. Starting in Colorado, Metrc overcame these challenges by developing three different tag types: Medical, Adult-Use, and Hemp. They are color coded and allow both the licensees and regulatory agency to easily differentiate by sight between a tagged Medical product versus Adult-Use or Hemp. Metrc has also developed different templates that give users increased efficiency in packaging and transferring these products between co-located facilities.

Out-of-State Patients: Within jurisdictions that allow for reciprocity with other state medical cannabis programs, there were challenges in verifying out-of-state patient ID cards. The system was originally designed to validate in-state patients directly from the patient registry integrations that were in place. The District of Columbia was the first client agency of ours to address this. Together, we determined that the patients would have a separate verification process in our System. The agency staff and licensees would create an "External Patient," and this allowed for easy reporting of these patients so that the agency could investigate suspicious behavior and report the reciprocity patient numbers along with the verification method.

Substitute Codes: One of the most unique requests that our team has experienced was the need to associate a cannabis product with a substitute National Drug Code (NDC) in Ohio that would be automatically generated by the Metrc System. (The NDC was required for Ohio's Prescription Monitoring Program.) To achieve this, we created our most customized development item during any deployment: the "Item Approval Process." This process allowed the jurisdiction to review, comment on, and approve any product that was created by a licensee directly within the System. Once approved, the System would assign a unique identifier directly to the item created, serving as a substitute of the traditional NDC code.

Incumbent Vendor Replacement: In both Nevada and Maine, state regulatory agencies requested that Metrc take over the seed-to-sale contract from an incumbent vendor. Because of the importance of getting a replacement system up and running as soon as possible, Metrc stepped in and launched our system in record time, within 60 days, for State and licensee use in both jurisdictions. To date, Metrc is the only track-and-trace vendor that has been requested to replace an incumbent vendor, demonstrating the trust and commitment to performance that we have developed with the regulatory community. Additional information on these two projects is included in **Attachment 3** and **Attachment 4**.



Employee Badging: During an implementation effort in Maryland, it was identified that the agency did not have the ability to print physical badges for their licensed employees. Metrc worked with the licensing vendor to provide a badge printing system to support this unique requirement that was unable to be fulfilled by the licensing system alone.

Flight Transport: Metrc's built-in transport manifest was designed for product transportation by land (e.g., by automobile). However, given Alaska's unique geography, transportation by land was not always feasible: distances between cities are often too great, and ice roads and other infrastructure may not be available year-round. To address this, Metrc adjusted our transport manifest to accommodate product transfers by air (i.e., by plane). This enabled our client agency, the Alcohol & Marijuana Control Office, to facilitate and monitor marijuana transportation in a novel way.

Licensee Credentialing: In the summer of 2021, licensees in Oklahoma were nearing the regulatory deadline to begin tracking product in the Metrc System. Unfortunately, most licensees had not yet taken a training course and were not yet approved to use the System. What followed was a massive rush to take Metrc's introductory training course and gain access to the System. Metrc support and training worked overtime to ensure that over 10,000 licensees were adequately trained and granted access to the system. Between March and April, Metrc hosted 10 classes per week, with an average of 500 licensee users trained per day. In that same timeframe, we credentialed an average of over 150 licensee admins per day, granting them access to the System and the ability to add and manage users associated with their business license.

Internet Connectivity: Also in Alaska, regulators were concerned about the lack of internet connectivity in some communities. Since Metrc is a cloud-based solution, this meant that licensees without reliable internet connectivity might become noncompliant with reporting requirements. To address this, Metrc developed a template CSV file so that licensees could document supply chain events offline, record it in the file, and upload it to the Metrc System at a later time when they were able to connect to the internet.

Adult-Use Expansion: Having already provided our seed-to-sale solution for Michigan's medical market for two years, our client agency, the Marijuana Regulatory Agency, tasked Metrc in 2019 with expanding our solution in to serve the recently legalized adult-use market. With adult-use slated to begin in January 2020, Metrc successfully implemented our System a month ahead of schedule, enabling adult-use sales to begin early in on December 1, 2019.

With all of the programs Metrc works with, we recognize the need for enhancements or improvements as each program matures with deeper understandings of the cannabis industry. Our biggest takeaways with the work we have done is to remain flexible and configurable with all our work and ensure proper communication is established between all stakeholders (regulatory agency, licensees, and third-party vendors) when any System changes or processes occur.



IV.b. Response to Software Requirements

Metrc's responses to RFP Sections 3.1 – 3.5 requirements are below each stated requirement, in dark green font.

IV.b.1. Cultivator and Manufacturer Tracking and Inventory

3.1a: Inventory Information Tracking

The system must provide cultivators and manufacturers the ability to define inventory of plants, strains, clones, seedlings, and cannabis product. The information that must be tracked in the system are including but not limited to the following:

- *Unique identifiers for individual plant;*
- *Quantity and form of cannabis maintained by the establishment at the facility in the appropriate units of measure determined by the State;*
- *The amount of plants being grown at the facility;*
- *The amount of plants being processed at the facility; and*
- *Any other information required by the State*

The inventory record must reflect destruction or disposal of cannabis waste, theft, and transfer record.

The Metrc System provides cultivators and manufacturers the ability to define inventory of plants, strains, clones, seedlings, and cannabis products. The System tracks all State required information including quantity and form of cannabis maintained by the establishment at the facility in the units of measure determined by the State and the amount of plants growing or being processed at the facility.

Real-Time, End-to-End Track and Trace

Cultivators and manufacturers will input plant information at each phase of growth and processing, as described in the following paragraphs and demonstrated in Figure 3.

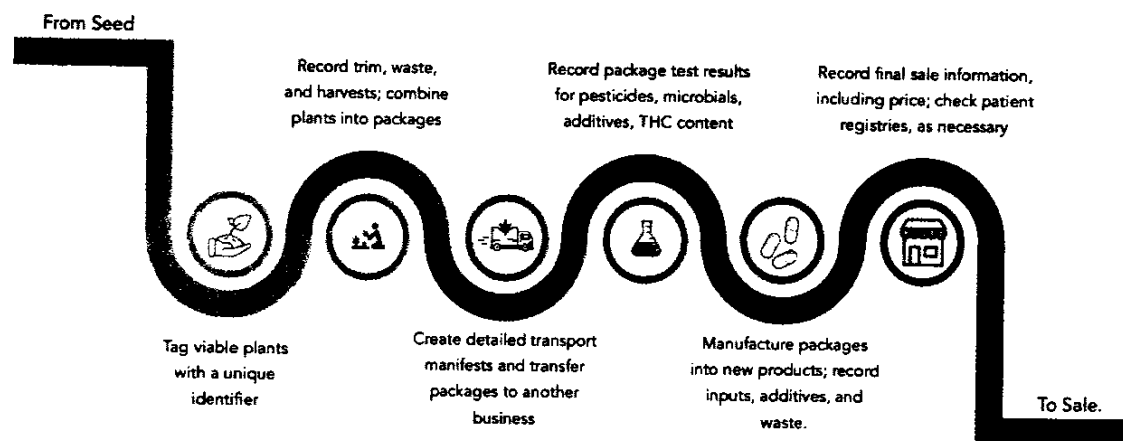
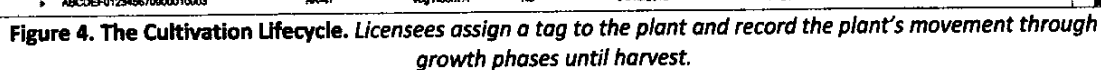


Figure 3. Real-time, End-to-End Tracking. *The State receives granular details about the marijuana lifecycle, all the way back to the original source.*

The cultivation lifecycle is captured in a set of events based on growth phases and plant location. First, the cultivator affixes a Metrc Radio Frequency Identification (RFID) tracking plant tag to every seedling when they become viable, thus tracking every plant grown from seed or clone. As the plant grows and matures, the System captures key measures such as varietal type, height, weight, trim, and waste during each phase of the growing process—information that is forever tied to that plant’s unique identifier (Hex-ID). If a cultivator is storing seeds on premises prior to reporting them as an immature plant batch intended for growth, they affix an RFID tag to the stored seeds. The State determines how they want to configure the System for how the seeds are to be reported (either as individual unit counts of seeds or the total seed weight).

Ultimately, plants are harvested and the flower is combined, cured, and moved between rooms, facilities, etc. and potentially processed into new products, such as concentrates. The System captures each of those events and associated information, including all the State-required harvest and product processing data: harvest data (e.g., strain, marijuana wet weight, marijuana dry weight, other material wet weight, other material dry weight, location of harvested material, time and date of harvest, and waste); product processing data (product type, quantity, weight, volume, waste, manufacture date, and expiration date, if applicable) (see Figure 4).



The product's final sale to a consumer closes the loop on the plant's history, providing proof of sale for tax revenue and reporting. In this way, every action that changes the form, location, or custody of cannabis material is dated, logged, and stored in the System for reference by the State and regulators.

Supply chain events are captured using an RFID (radio frequency ID) tag and Hex-ID (unique identifier) that Metrc creates specifically for and assigns to each licensee (see Figure 5).

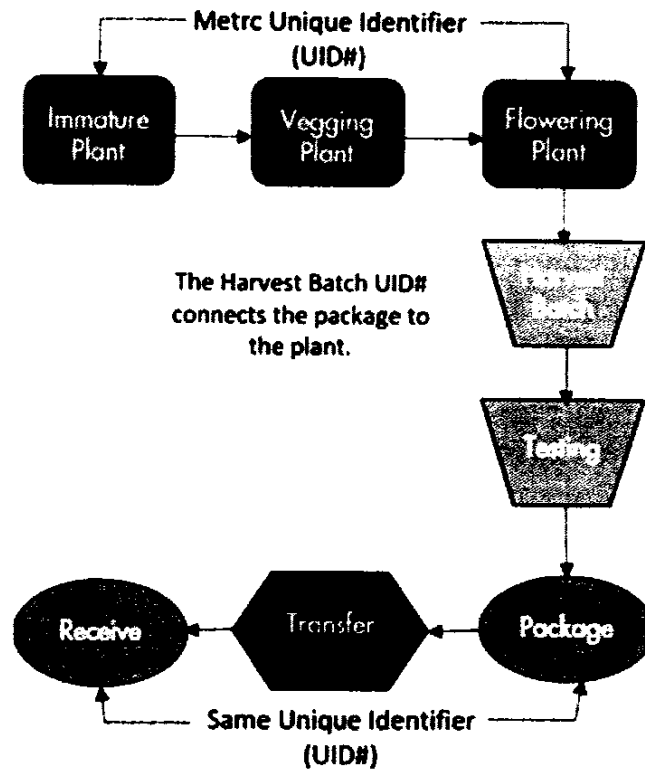


Figure 5. Chain-of-Custody Tracking. *The State tracks every event in the product lifecycle in real time—the System tracks over 370 unique supply-chain events.*

Licensees attach MetrC’s unique, non-repeating RFID identifier tags to each of their viable plants, and as it is grown, trimmed, harvested, and moved, they enter data, including weight (wet and dry), strain, location, date and time, waste, and additives, into the System. These actions are recorded as independent events associated to each plant, harvest, package, transfer, etc. As the cannabis plant moves through production, supply chain events are continuously documented by the licensee.

Destruction or Disposal of Waste

The System allows for cultivators and manufacturers to designate any unsuitable product as waste and to denote how it will be disposed of. When users record waste in the System, they select from a predetermined list (e.g., Landfill, Unusable, etc.), which MetrC can configure to the State’s requirements. These categories allow the State to have consistent reports on all waste destruction. The State can maintain the categories in the administration section of the System.

The System tracks waste in three areas of the System: Pre-harvest Waste (recorded via plant or room location), Harvest Waste (recorded by batch), and Package Waste (recorded via adjustments with reason codes assigned by the State).



Furthermore, Metrc can configure the System to keep licensees from transferring waste to other licensees. We develop these types of configurations during implementation in collaboration with the State to ensure that the System adheres to South Dakota's rules and laws.

Theft

The System allows cultivators and manufacturers to report when cannabis is lost, stolen, or diverted. When such an event happens, users input an inventory adjustment, citing pre-set reasons determined by the State. In addition to "adjustment reason," users provide other information (as desired or required by the State) including Package ID, Adjustment Quantity, Adjustment Unit of Measure (e.g., weight, units, or volume), Adjustment Date, and Note. Adjustments automatically trigger a real-time notification based on State configurations, alerting the State when cannabis is lost, stolen, or diverted.

Transfer Record

The Metrc System provides a complete and thorough transfer manifesting process and enables the State to require the cultivator or manufacturer to enter select information about the transfer. All transfers are created, viewable, and received in the System, and inventory is moved from one licensee to another in the System to maintain the chain of custody.

When transfers are initiated, the System creates a transport manifest that includes fields for licensee identification, source facility, destination (another licensee), product ID and lot number, quantity, and units of measure (including gross and net weights), departure time and arrival, driver and vehicle information (e.g., driver's name and license number and car make and model), and route. The transfer must include packages from the original licensee's inventory.

Once the required information is entered, the System automatically generates a transfer manifest containing the details about the transfer and licensees involved, populating all of the license information, such as address. The manifest can be printed and kept with the packages through the transfer process.

When the transfer arrives at the receiving licensee, that facility can accept the transfer and all the contents directly into its inventory. This step ensures that the chain of custody is maintained, and all product is accounted for throughout the transfer.



3.1b: Inventory Record Updates – Cultivator

The system must allow the inventory record to be updated each time:

- 1. A seedling exceeds its size limit determined by the State and is considered a plant;*
- 2. A plant flowers for the first time;*
- 3. A plant is trimmed or harvested;*
- 4. A testing batch is created; or*
- 5. Cannabis is packaged for retail sale.*

The record of cannabis packaged and labeled for transfer must include the number of marketing layer, and quantity of cannabis in each marketing layer.

Record Updates

Inventory can be updated to record all events described in this requirement, and many more. In total, the System captures over 370 unique production events and related information. The System uses RFID, a barcode, and a unique number identifier (Hex-ID) to track cannabis through every phase of the supply chain in real time. It requires licensees to input plant information at each phase of growth (including conversion from seedling to immature plant, flowering plant, harvesting/trimming of plants) and captures chain of custody information for each step of the process. As the plant grows and matures, the System captures key measures such as varietal type, height, weight, trim, and waste during each phase of the growing process—information that is forever tied to that plant's unique identifier (Hex-ID).

Testing Batch

When a licensee creates a lab test sample, they can select a Lab Test Batch from a predetermined list. Lab Test Batches are normally determined by regulatory department rules or statutes (e.g., pesticides). The State maintains the batches in the administration section of the System.

Packaged for Retail

Cultivators can use the Metrc System to split packages for retail and keep the inventory up to date. The System has two package types: the original package created from a harvest and new "repack" packages (see Figure 6). Packages can be combined or divided up to create a new package. The new package option enables cultivators to record any configuration of new package that exists in the marketplace. It allows cultivators to split a given cannabis product lot for distribution to multiple retail outlets. Each package tracks the number of marketing layers it contains—as well as the quantity of cannabis in each marketing layer. For example, a package in Metrc might consist of 100 boxes of chocolate brownie edibles, and each box might include 10 edibles, each with 10 milligrams of THC.

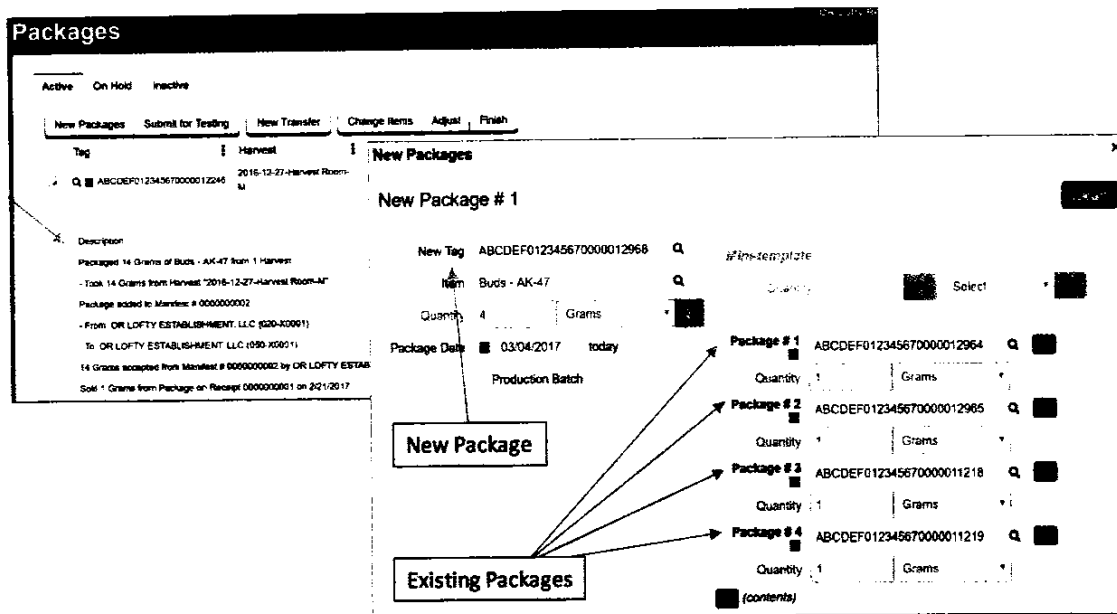


Figure 6. Built in Splitting Functionality. Cultivators can easily split a package while preserving complete granular product tracking and tracing.

Each time a cultivator repacks product in the System, they must place a new RFID package tag on the new package.

3.1c: Inventory Record Updates – Manufacturer

The system must allow the inventory record to be updated each time:

1. A quantity of extract or concentrated cannabis is made from cannabis flower or trim;
2. A quantity of cannabis product is made from concentrated cannabis, cannabis extract, flower, or trim;
3. A quantity of cannabis product is packaged for retail sale.

The record of cannabis packaged and labeled for transfer must include the number of marketing layer, and quantity of cannabis in each marketing layer.

To update their inventory records, manufacturers would record updates in the same manner described above for cultivators. The System enables manufacturers to input and record each stage and all details described in this requirement.

Record Updates

Inventory can be updated to record all events described in this requirement. The System uses RFID, a barcode, and a unique number identifier (Hex-ID) to track cannabis through every phase of the supply chain in real time. It requires licensees to input plant information at each phase (including extract or concentrated cannabis from flower or trim and cannabis product made from concentrated cannabis, extract, flower, or trim) and captures chain of custody information for each step of the process. The System captures key data, such as quantities as the plant's



flower or trim is used for extractions or concentrated cannabis and when cannabis product is created—information that is forever tied to that plant’s unique identifier (Hex-ID).

Packaged for Retail

Manufacturers can use the Metrc System to split packages for retail and keep the inventory up to date using the same process as cultivators use for the same function. The System has two package types: the original package created from a harvest and new “repack” packages. Packages can be combined or divided up to create a new package. The new package option enables manufacturers to record any configuration of new package that exists in the marketplace. It allows manufacturers to split a given cannabis product lot for distribution to multiple retail outlets. Each package tracks the number of marketing layers it contains—as well as the quantity of cannabis in each marketing layer.

3.1d: Inventory Record Updates - Testing Facility

The system must maintain and update an electronic copy of the following information:

- 1. All samples in its possession with unique identifiers and quantities expressed in units specified by the State; and*
- 2. All other cannabis, cannabis extracts, and cannabis products acquired*

The inventory record should reflect:

- *The quantity of each sample rendered unusable by testing;*
- *The quantity of each sample returned to the establishment;*
- *The quantity of each sample destroyed or disposed of; and*
- *The quantity of any sample lost, stolen, or otherwise unaccounted for.*

The testing facility would be able to provide a point in time inventory report to reflect all samples, cannabis extracts, cannabis products, and all other cannabis in its possession with unique identifiers (Hex-ID) and quantities expressed in units. To update their inventory records, testing facilities record updates in the same manner described above for cultivators and manufacturers. The System enables testing facilities to input and record details described in this requirement including the quantity of samples rendered unusable; the quantity of samples returned to the establishment; the quantity of destroyed or disposed of samples; and lost, stolen, and unaccounted for samples.

Unusable or Destroyed Samples

The System allows for testing facilities to designate any unsuitable product as unusable, to denote how it will be disposed of, and to record the quantity. When users record waste in the System, they select from a predetermined list (e.g., Landfill, Unusable, etc.), which Metrc can configure to the State’s requirements. These categories allow the State to have consistent reports on all waste destruction. The State can maintain the categories in the administration section of the System.



Metrc can also configure the System to keep licensees from transferring waste to other licensees. We develop these types of configurations during implementation in collaboration with the State to ensure that the system adheres to South Dakota's rules and laws.

Lost, Stolen, and Unaccounted for Samples

The System allows testing facilities to report when cannabis is lost, stolen, or diverted. When such an event happens, users input an inventory adjustment, citing pre-set reasons determined by the State. In addition to "adjustment reason," users provide other information (as desired or required by the State) including Package ID, Adjustment Quantity, Adjustment Unit of Measure (e.g., weight, units, or volume), Adjustment Date, and Note. Adjustments automatically trigger a real-time notification based on State configurations, alerting the State when cannabis is lost, stolen, or diverted.

Returned Samples

To record and track product returns, the testing facility utilizes the repackage functionality used by cultivators and manufacturers as described in 3.1b and 3.1c to create a new package with the product to be returned to the originating facility. They then return the item using the transfer manifest. The originating facility accepts that returned product, and the chain of custody is maintained.

Packaged for Retail

Manufacturers can use the Metrc System to split packages for retail and keep the inventory up to date using the same process as cultivators use for the same function. The System has two package types: the original package created from a harvest and new "repack" packages. Packages can be combined or divided up to create a new package. The new package option enables manufacturers to record any configuration of new package that exists in the marketplace. It allows manufacturers to split a given cannabis product lot for distribution to multiple retail outlets.

3.1e: Inventory Reconciliation Cannabis

Establishments will reconcile their physical inventory with the information in the system at the end of business each day. Inconsistencies will flag the department for further investigation. Reconciliation items will include the following:

- *Plant material at the facility;*
- *Plant material in transit; and*
- *Any other information required by the State*

Establishments can reconcile their physical inventory with the information in the Metrc System by running an inventory point-in-time report, which is accessed through the report dashboard. At a minimum, this report captures active plant material at the facility and plant material in transit. The State can run the report for any window of time it needs to be generated for.



If there are discrepancies, establishments can then use the Adjust Packages functionality, which allows the user to input inventory adjustments for reasons permitted by the State. Data input includes the following fields: Package ID, Adjustment Quantity, Adjustment Unit of Measure, Adjustment Reason (predefined by the State), Adjustment Date, and a required notes field based on the State's configuration. Alerts can be easily set up in the System so that specific events, such as inventory adjustments, can automatically trigger a notification to the State.

If an establishment runs into an issue while reconciling their physical inventory, they will be able to turn to one of our specialized support teams, the Reconciliation Team, for support. The Reconciliation Team provides guidelines from the regulator to help licensees cleanup their Metrc System accounts. Members of the Reconciliation Team answer questions for establishments and work with the regulators' investigators to make sure cleanup is performed within the jurisdiction's guidelines. This valued service helps establishments and investigators efficiently update records in the System.

3.1f: Daily Transfer Record

The system must maintain and update by midnight an electronic record of all cannabis including seeds, plants extracts, or products obtained by a cardholder or another establishment, and all cannabis transferred to another establishment. The transfer record must meet the following requirement:

- 1. It must use the same units of measures as the inventory record; and*
- 2. It must reflect all transport manifest, purchase orders, and requisition forms*

The System maintains and updates an electronic record of all cannabis including seeds, plant extracts, or products obtained by a cardholder or another establishment for all data entered into the System by midnight every evening. The System provides detailed status reports at every point during the growth, harvesting, transporting, sales and lab testing reports for both the State and licensees. Standard reports from the control panel include harvest, plant inventory, monthly plant inventory, plant trend, wholesale transfer, cultivation transfer, starting wet weight of harvest and total package adjustment reports.

The System maintains and updates, by midnight each night, an electronic record of all cannabis transferred to another establishment. The transfer record will use the same units of measures as the inventory record and will reflect all transport manifests. All transfers are created, viewable, and received in the System, and inventory is moved from one licensee to another in the System to maintain the chain of custody.

When transfers are initiated, the System creates a transport manifest that includes fields for licensee identification, source facility, destination (another licensee), product ID and lot number, quantity, and units of measure (including gross and net weights), departure time and arrival, driver and vehicle information (e.g., driver's name and license number and car make and model), and route. The transfer must include packages from the original licensee's inventory.



Once the required information is entered, the System automatically generates a transfer manifest containing the details about the transfer and licensees involved, populating all of the license information, such as address. The manifest can be printed and kept with the packages through the transfer process.

When the transfer arrives at the receiving licensee, that facility can accept the transfer and all the contents directly into its inventory. This step ensures that the chain of custody is maintained, and all product is accounted for throughout the transfer.

While the System does not currently create or house purchase orders or requisition forms, the majority of the required functionality and data capture is included in our External Incoming Transfer process. External transfers allow for a licensed facility to designate a transfer of inventory that is coming from the unlicensed marketplace, such as patient donations. These transfers are designed to be flexible to the State's unique rules and are based on selectable fields that the State can configure, such as including license number or cardholder identification number. Metrc will work with the State during our configuration build-out and make updates to our system to ensure we accommodate all State-required functionality, such as the generation of a unique requisition form. Also see our responses to 3.1o and 3.1p, below on page 61.

3.1g: Pesticides Tracking

The system must provide the establishment the ability to track and any pesticides used during production. The following items will be recorded in the system:

- *The date of pesticides being applied;*
- *The name of the employee applying the pesticides;*
- *The name of pesticides that was applied;*
- *The amount of pesticides applied;*
- *The unique identifier or the batch number of plants that received the application; and*
- *A copy of the label of the pesticides applied*

Establishments record and track every inventory transaction (event) throughout the supply chain, including pesticides, either directly through the online user interface or via API integration. Establishments input plant information including additives (e.g., pesticides, fungicides, growth regulators) and waste, along with required information such as the name of pesticides applied and the amount of pesticides applied at each phase of growth, and the System captures chain of custody information with date and time stamps and the personnel involved in each step of the process. The System's unique number identifier (Hex-ID) tag is used to track cannabis through every phase of the supply chain in real time.

While the System does not currently store a copy of the label there is functionality to allow the licensee to enter label information such as product name, EPA registration number, supplier, and all ingredients. Metrc will update our system to accommodate additional State needs to meet this requirement. We look forward to further discussing the approach, timeline, and specifics with the State.



3.1h: Lab Testing

The system must be able to track sample procurement, sample origin, testing stages, testing results, and alert the State upon testing failure. The system must be able to record all of the following attributes of any plant or product:

- *Cannabinoid Potency;*
- *Microbials;*
- *Heavy metals;*
- *Solvents;*
- *Pesticides; and*
- *Any other attributes required for testing by Administrative Rules*

The testing results and record can only be added by an agent of testing facility, and the record should not be editable by agents of other establishment types.

The System tracks lab testing, including sample procurement, sample origin, testing stages, testing results and currently tracks many different aspects of the plants and strains including but not limited to cannabinoid potency, microbials, heavy metals, solvents, CBD, THC, waste, Indica and Sativa percentages, pesticides, and other data elements. Metrc can configure additional fields and tracking capability for growth regulators, soil, or other materials defined in a discovery process with minimal effort.

The Metrc System has robust functionality around product testing. Establishments can create a test sample package of small amounts of product from the source harvest or package and send it to a testing lab for testing (see Figure 7). Tracked data elements include date/time of transfer, transferred by, order number, source license number, laboratory name, laboratory license number, and a list of transferred products including product ID, product name, batch number, weights, and quantity. The System also captures the identification of the people who created the package, shipped the package, and received the package.



Record Tests

Test Package # 1

Package: 1A4FF03000000026000000004 **Mini-template**

Result Date: 01/03/2018 **today**

Test Batch: **Select**

Test Result Tracking

Selecting a Test Batch Adds One or More Tests

Category I Residual Tests (not required)
 Category II Residual Solvents and Processing Chemicals
 Category III Residual Pesticides
 Category IV Residual Solvents and Processing Chemicals
 Foreign Materials (optional)
 Heavy Metals (optional)
 Heterogeneity (edibles)
 Microbiological Impurities (Aspergillus)
 Microbiological Impurities (required)
 Moisture Content and Water Activity
 Mycotoxins (optional)
 Terpenoids (optional)

Result # 1 Escherichia coli (pass/fail)

Test Result: **0.0001**

Status: ☒ Passed ☐ Failed

Notes: **Notes can also be recorded.**

Result # 2 Salmonella spp. (pass/fail)

Test Result: **0.0001**

Status: ☒ Passed ☐ Failed

Notes: **Notes can also be recorded.**

(results)

Cancel

Figure 7. Test Packages and the Test Results. *The State has full testing visibility and flexible testing opportunities.*

Testing results and records can only be added by a testing facility agent and cannot be edited by agents of other establishment types.

In the case of testing failures, the State can specify if and how product can be remediated, the requirements for doing so, and the notifications and identifiers. For example, if a licensee's product failed for water activity (meaning the flower was too wet), the licensee could remediate by allowing the flower to dry longer and retest. If it failed for mold on flower or trim, the licensee could remediate by extraction process. If a product has failed testing at any capacity, the System can require the failed product to either be remediated and retested or even destroyed (depending on the State's rule). The System can also be configured to prevent the ability for failed product to be put onto a transfer manifest and moved to another establishment, if desirable for the State.

Alerts

The System can flag, via alert or notification, when any product fails testing or does not meet State standards by citing the specific component of failure. If a product has failed testing at any capacity, the System can require the failed product to either be remediated and retested or even destroyed (depending on rule). The System can also be configured to prevent the ability for failed or untested product to be put onto a transfer manifest and moved to another establishment.



Record

The System records the lab's test results, and results are searchable and sortable by package, harvest, test type, test status, test date, facility (lab or licensee), and any other tracked field. Test results are uploaded by the lab and can be exported or downloaded in Microsoft (MS) Word, MS Excel, and file formats such as CSV or PDF.

3.1i: Testing Sample Record

The system must allow establishments to assign the following identifier to samples being submitted to the testing facility:

- 1. A unique batch identifier to the cannabis, cannabis extract, or cannabis product being tested; and*
- 2. A unique sample identifier to each sample unless the sample is taken by an agent of the testing facility.*

The system must allow establishment to maintain an electronic copy of testing sample record that includes the following information:

- The batch identifier and quantity of each batch from which samples were drawn;*
- The identifier of each sample record, its quantity, and the batch identifier associated with the sample;*
- The tests to be performed;*
- Test results, including a note of whether the testing facility has indicated the batch is safe or unsafe for transfer; and*
- The quantity of each batch and each sample shall be expressed in the same units as the inventory record.*

The System must alert the State upon testing failure or products not meeting the standards set by the State.

Testing Sample Records

The System allows establishments to maintain electronic records of testing samples. Records include all required identifiers and quantities of associated samples (in appropriate units), tests to be performed, and test results. The System uses RFID, a barcode, and a unique number identifier (Hex-ID) to track marijuana through every phase and every event in the supply chain including testing.

In the case of testing failures, the State can specify if and how product can be remediated, the requirements for doing so, and the notifications and identifiers. For example, if a licensee's product failed for water activity (meaning the flower was too wet), the licensee could remediate by allowing the flower to dry longer and retest. If it failed for mold on flower or trim, the licensee could remediate by extraction process. If a product has failed testing at any capacity, the System can require the failed product to either be remediated and retested or even destroyed (depending on the State's rule). The System can also be configured to prevent the ability for failed product to be put onto a transfer manifest and moved to another establishment, if desirable for the State.

Test results are searchable and sortable by package, harvest, test type, test status, test results, test date, facility (lab or licensee), and any other tracked field. Test results are uploaded by the



lab and can be exported or downloaded in Microsoft (MS) Word, MS Excel, and file formats such as CSV or PDF.

The System can alert the State upon testing failure or products not meeting the standards set by the State. Additional information is included above in our response to 3.1h.

3.1j: Tracking and Disposal of Product

The system must allow cultivator or manufacturer to record disposal of unused, excess, or expired cannabis including returned cannabis products from dispensaries or Cannabis cardholder. The system also must record the disposal of cannabis product that failed to meet testing standards. The system must provide abilities to record, reconcile and maintain the following information:

- *The original tracking number at the time of the dispensing or the name of the patient if the tracking number is unavailable;*
- *The date the cannabis was returned or disposed;*
- *The quantity of cannabis returned or disposed;*
- *The type and lot number of the cannabis returned or disposed;*
- *Reason for disposal or return;*
- *Any other information required by the State*

The system must flag any inconsistencies or unreconciled record of returned or disposed cannabis product.

Unusable, Excess, Expired Cannabis

The System allows cultivators and manufacturers to designate any unsuitable product as unusable, to denote how it will be disposed of, and to record the quantity. The record of waste also includes return date, the quantity returned, and the unique ID of the package returned. When users record waste in the System, they select from a predetermined list of Waste Methods (e.g., unused, excess, expired, returned), which Metrc can configure to the State's requirements. These categories allow the State to have consistent reports on all waste destruction. The State can maintain the Waste Method categories in the administration section of the System.

Returns

To record and track product returns, the System captures the date of return and the quantity of product returned, the unique ID of the product returned, the item information as well as the user who completes the return in the System.

Alerts

The System can flag, via alert or notification, when any product is returned or wasted.



3.1k: Travel Manifest

The cultivator and manufacturer are required to generate transport manifest for transportation of cannabis to and from their facility, dispensaries, testing facility, a waste facility, and other location as approved by the department. The system must record and issue the travel manifest and generate copies of the manifest. The travel manifest should contain the following information:

- The information of establishment transporting cannabis or cannabis products including but not limited to license number;*
- The information of establishment receiving cannabis or cannabis products including but not limited to physical address;*
- Web address of the departments' secure verification system;*
- Description and quantities of all items in each transport;*
- Date of transport, and approximate time of departure and arrival date;*
- Vehicle make, model and license plate number;*
- The name and signature of driver;*
- The name and signature of the establishment agent accepting the transport;*
- Any other information required by State*

The Metrc System records and issues the required travel manifest and generate copies of the manifest. It can contain all required information. The System provides a complete and thorough transfer manifest process. All transfers must be initiated and received through the System. As inventory is moved from one licensee to another, the System tracks it to maintain the chain of custody.

Transfers must include packages from the original licensee's inventory. Licensees select the products and unit of measure that will be transferred from their current inventory; they also select a Transfer Type (e.g., Laboratory, Wholesale, Affiliated, etc.) from a predetermined list that is configured by the State. The System also allows the State to require additional information about the transfer, such as driver/vehicle information and contact, planned route, and sale price.

Once required information is entered, the System automatically generates a transfer manifest containing the details about the transfer and the facilities involved (see Figure 8). The manifest is saved in the System and is printable and viewable in the System by both the shipping and the receiving establishment. Other information includes ship from name, license number and route description; destination address, name, license number, and address; and shipment product description, product ID, batch number, test results, quantity, and units of measure, including gross and net weights.



The System enables establishments to record the cannabis that is received as inventory. When the product arrives at the receiving establishment, that licensee compares the manifest to the product received, then uses the System to formally accept it into their inventory and take custody of it, both physically and in the System. In this way, all deliveries are tracked and recorded as inventory once received.



3.1m: Sales and Distribution Record

The cultivator and manufacturer will maintain complete and accurate electronic sales transaction records in the department's tracking system, including the following item;

- *The date of each sale and distribution;*
- *The item number, product name and description, and quantity of cannabis sold or otherwise distributed;*
- *The sale price; and*
- *Any other information required by the State*

The System enables cultivators and manufacturers to maintain complete and accurate electronic sales transaction records. The time and date of sale and distribution, price, license number, order number, sales items, weight or volume of product dispensed, and any other fields required by the State will be included in the details of the transaction. Transaction data also includes adjustments, such as for refunds, credits, and voids.

The Metrc System captures and maintains accurate and detailed sales transactions. The System generates a unique tracking number (receipt ID) for each sale and dispensing transaction. Each transaction is recorded by package in the System using the unique identification number (Hex-ID) assigned to the package when it was tagged and inputted into the System. This technology allows the sold or dispensed product to be traced back to the certificate of analysis generated and stored within the System by a testing lab.

3.1n: Recall Mechanism for Manufacturer

Manufacturer may need to recall cannabis. The system should provide a mechanism to document any recalled product, reason for recall, date of recall, and relevant unique identifier for the batch or lot numbers. The system should also flag the State personnel for any recall actions taken by manufacturers within the system.

In the event that the manufacturer needs to recall cannabis, the System provides a mechanism to document any recalled product, reason for recall, date of recall, and relevant unique identifier for the batch or lot numbers.

The Administrative Hold tool provides regulators with the ability to hold packages from being transferred out of a license until they have completed an action (investigation, recall, etc.). This functionality is flexible in that it can be as granular as a single package, plant, or harvest batch and as widespread as an entire license. The State can also place a "global hold" on a package, which puts on hold any package that was derived from it down the supply chain, even if those packages are in a different license. This allows the State to place packages affected by a recall on hold quickly and efficiently while also alerting the licensees to the hold through banner notifications.

The Package Trace is a core component within the System that provides regulators the ability to trace a specific package's source and derived packages throughout the entire supply chain within seconds. This feature allows regulators to take a package of product in any license and



follow all its collective touchpoints through any other license, all the way back to the plants used in its production.

Each package has a set of tracked events recorded by its unique identification number. These events chronicle the history of each package. Package Trace, however, is a genealogy of a package based on all associated events. If a portion of a package was packed into another package and then a portion of that package was repackaged, all those events are part of the first package's trace. Package Trace is launched from a searchable grid that organizes trace data into a graphical hierarchy.

With this tool, regulators can pinpoint every package that has been affected by a tainted element in the event of a recall.

3.1o: Requisition Form

The system must create a requisition form when a cultivation facility accepts cannabis from a cardholder at no value. The form must contain the cardholder's identification number and acknowledgement signature from cardholder that nothing of value was received in exchange of the cannabis.

As mentioned in 3.1f, the majority of this functionality and data capture exists within the System as External Incoming Transfers. Metrc will work with the State during our configuration build-out and make updates to our system to ensure we accommodate all State-required functionality, such as the generation of a unique requisition form.

3.1p: Purchase Order

The system must create a purchase order when a cultivation facility purchase seeds from a cardholder. The form must contain cardholder's identification number, quantity of the seeds, value exchanged, and the acknowledgement signature from the cardholder.

As mentioned in 3.1f, the majority of this functionality and data capture exists within the System as External Incoming Transfers. Metrc will work with the State during our configuration build-out and make updates to our system to ensure we accommodate all State-required functionality, such as the generation of a unique purchase order form.



"Metrc has been a true partner in helping our businesses stay compliant in Colorado and Oklahoma. Protecting the integrity and safety of Apothecary products for our patients and customers is my number one goal, and Metrc helps me do that every day with intuitive software, great support, and training when we need it. And we love the RFID capability. At our grow in Oklahoma, we're caring for up to 15,000 plants at a time, and we rely on RFID to know precisely what is growing where, improving our operating efficiency. I enthusiastically recommend Metrc as a regulatory partner. I am also happy to answer any questions about how Metrc has helped my business and how it can support better regulatory outcomes in South Dakota."

- LeeAnn Weibe, CEO of Apothecary Farms

3.1q: Travel Manifest Approval (Optional)

Each transport should be approved electronically or in writing by an authorized employee of the establishments when departing the facility and by an authorized employee of the receiving establishment or waste facility. The system must allow authorized employees of the receiving establishment to review and verify the type and quantity of the transported cannabis or plant material against the information on the travel manifest prior to signing the travel manifest. If the approval process is in writing, the system should have the document upload functionality so the copy of the approved travel manifest is uploaded into the system.

The System supports the transport of product between licensed businesses and allows for the jurisdiction to require the licensee to enter select information about the transfer such as transporting license, agent information and contact, planned route, and wholesale price. The transfer must include packages from the original license's inventory.

Once the required information is entered, the system automatically generates a transfer manifest containing the details about the transfer and licensees involved populating all of the license information such as address. This manifest can be printed and kept with the packages through the transfer process.

When the transfer arrives at the receiving license, that facility can inspect the packages and accept the transfer and all the contents directly into its inventory. This step ensures that the chain of custody is maintained, and all product is accounted for throughout the transfer. In the event that the receiving facility is unable to accept the manifested packages, they can reject the items and select the reason for rejection. This will create a return manifest to the originating facility.



While this method currently allows the electronic acceptance of manifested packages, there is currently no document upload functionality. Metrc looks forward to further discussing this requirement with the State and how we might meet it through system modification.

3.1r: In-Transit Documentation (Optional)

The system should have the ability for establishment agents who are transporting cannabis on public roads to record the following information:

- 1. Travel routes taken to deliver products to establishments;*
- 2. Refueling and all other stops in transit, including reason, duration, and location of the stop.*
- 3. Any traffic stop, breakdown, or collision involving a vehicle being used by an establishment to transport cannabis or cannabis product.*
- 4. Any theft or break-in involving a vehicle being used by the establishments to transport cannabis or cannabis product.*

The System allows the State to require additional information about the transfer including information about travel routes, refueling and other stops, traffic stops, theft or break ins, and more. During manifest creation, the licensee is able to add details about the planned route to that section of the Transfer. This same input field could later be edited to include details about refueling, thefts, breakdowns, or collisions.

For details about our transfer manifest, please see 3.1k, on page 58, above.

3.1s: Product Labeling (Optional)

The system should allow the manufacturer to create and print labels for the cannabis products. The label must include:

- List of any pesticides used in cultivation;*
- List of all ingredients and any gases, solvents, or other chemicals used in extraction;*
- List of major allergens including milk, egg, fish, crustacean shellfish, tree nuts, peanuts, and soybeans;*
- Net weight or volume of the cannabis or cannabis product*
- Equivalent cannabis weight (See Requirement 3.1v)*
- The length of time that it may take the patient to feel effects;*
- The length of time the patient should expect the result to last;*
- The weight label must have the flexibility for unit size (serving size, weight of concentrate...etc.) based on the product type;*
- Nutritional fact panel;*
- Any symbol developed by State to indicate the availability of THC;*
- Warning statement in font no smaller than 6 point font, " For use by qualifying patients only";*
and
- Any other information required by the State*



Additionally, the following test results can be listed on the label if the test was performed by registered cannabis testing facility:

- *Absence of Microbials;*
- *Absence of heavy metals;*
- *Absence of solvents;*
- *Absence of pesticides; and*
- *Potency*

The font size for the label shall be no smaller than 6 point font (1/12 inch).

The System provides an open, secure, and web-based API (Application Programming Interface) for integration of external information systems, data, and hardware. We have a well-established program for working with and validating third-party software providers (third-party vendors or TPVs) that integrate into the System's API and offer enterprise solutions to licensees.

Over 500 software providers have integrated into the Metrc System, including point of sale (POS), grow management, enterprise resource planning (ERP), laboratory inventory management (LIM), and other data systems. For example, Canix offers licensees both software and hardware (including product label printers) that integrate into the Metrc System (see Figure 9).

Figure 9. Canix's Label Printing Solution. Licensees and third-party vendors can integrate into Metrc to pull any required information in the creation of product labels.

Integrators and licensees alike will be able to pull any tracked information from the System for use in printing on labels. If the State desires this information to be presented, saved, or accessed in a particular format specifically for the production of labels, Metrc will be able to



update the System to accommodate this need. We look forward to further discussing the approach, timeline, and specific requirements with the State.

3.1t: Additives, Solvent, and Chemical Tracking (Optional)

The system should provide the establishment the ability to track any additives, solvents, and other chemicals used during production. The following items will be recorded in the system:

- *The date of additives, solvent, or chemicals being applied;*
- *The name of the employee applying the additives, solvent, or chemicals;*
- *The name of additives, solvent, or chemicals that was applied;*
- *The amount of additives, solvent, or chemicals applied;*
- *The unique identifier or the batch number of plants that received the application; and*
- *A copy of the label of the additives, solvent, or chemicals applied*

The System enables establishments to track any additives, solvents, and other chemicals used during production. As the cannabis plant moves through production, supply chain events are continuously documented by the licensee. Licensees input required information (as determined by the State) as they apply or use such items into the System. These actions are recorded as independent events associated to each plant, harvest, package, transfer, etc. We are currently developing new functionality to enhance the system's ability to capture the required steps of new product production.

3.1u: Quality Assurance (Optional)

The system should allow manufacturer to record all quality control procedures, and outcomes by batch and lot number in the system.

Metrc is currently developing new functionality to enhance the System's ability to capture the required steps of new product production. As part of that enhancement, the licensee would be able to record quality control procedures and record outputs by batch and lot number. This functionality should be available for Metrc users by the beginning of 2022.

3.1v: Equivalent Dosage (Optional)

The system should be able to calculate equivalent dosages based on the equivalency table provided by the State.

The Metrc System can calculate equivalent dosages based on the equivalency table provided by the State. The System can calculate equivalency between dosages, such as dried usable marijuana, wet-weight marijuana, edibles, concentrates, and extracts. It can also calculate by yield, potency, and market price, as the State desires.

This area is among those that are configurable by the State. We will work through this with the State to meet the regulations.



3.1w: Establishment Room Designation and Configuration (Optional)

The system should provide the establishments the ability to track plants through each growth phase by associating the individual plants with a particular room. Batches and partial batches will be tracked in the system.

The cultivator and manufacturer will record any removal of plants from a batch including the reason for removal.

The system must provide cultivators and manufacturers the ability to define and designate growing and production rooms. Rooms are including but not limited to the following:

- Germination;
- Vegetative;
- Flowering;
- Trimming;
- Curing;
- Processing;
- Packaging;
- Extraction; and
- Storage

Room Designation

The System enables establishments to track the entire growth process of plants and associate individual plants with physical locations. For indoor growers, this might be a room name, whereas for outdoor growers this might designate a plot name. Room designations can include Germination, Vegetative, Flowering, Trimming, Curing, Processing, Packaging, Extraction, and Storage. The System captures granular events as plants are harvested and the flower is combined, cured, and moved between rooms, facilities, etc. Every action that changes the location, form, or custody of cannabis material is dated, logged, and stored in the System for reference by the State and regulators.

Plants can be tracked as they are moved from room to room. The System allows the movement of immature, vegging or flowering plants in between rooms or locations by selecting the plants (by unique ID number) and selecting the change room button. Plants can be moved in large groups or individually. All plant movements are captured within the facility and includes date and time stamps with the name of the individual performing the move.

Locations are created by the licensing facility and include Name and Location type. Location types are defined by the State under the Administration drop down. We will work with the State to configure this.

Removal of Plants

Establishments record the removal of plants using the Report Waste functionality, which allows them to input inventory adjustments by selecting a waste type. Waste types are determined by the State. After selecting the waste type, they enter the waste weight and waste date. The State can receive notifications when waste is reported from harvest.



IV.b.2. Dispensary Tracking and Inventory

3.2a: Inventory Record Updates – Dispensary

The system must maintain and update an electronic copy of all cannabis and cannabis products including the type of products, testing batch identifier, the number of marketing layers, and the quantity of cannabis in each marketing layer.

The inventory record should reflect:

- 1. Any cannabis and cannabis products received from another establishments;*
- 2. Sales to qualifying cardholders including the cardholder's identification number;*
- 3. Returns of merchandise from cardholders, whether to be resold, returned to another establishment, or destroyed;*
- 4. Transfers to another establishment including returns; and*
- 5. Destruction of cannabis*

The Metrc System captures, maintains, and updates all required information, including the type of products, testing batch identifier, the number of marketing layers, and the quantity of cannabis in each marketing layer. The inventory record will include products received from other establishments, sales to cardholders including ID number, returns from cardholders, transfers, and destroyed cannabis.

Licensees report every supply chain event back to the State: plant life, waste generated, additives applied, package creation and distribution, transfers, retail sales, etc.

Dispensation and sales reporting is the final event in the chain of custody. It marks the last event in the tracing of each package and plant. The System generates a unique tracking number (receipt ID) for each dispensing transaction. Each sales transaction is recorded by package in the System using the unique identification number (Hex-ID) assigned to the package when it was tagged and inputted into the System. This technology allows the sold or dispensed product to be traced back to the certificate of analysis generated and stored within the System by a testing lab.

Returns

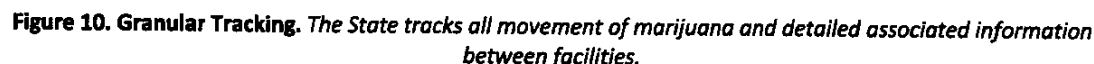
To record and track product returns, the System captures the date of return and the quantity of product returned, the unique ID of the product returned, the item information as well as the user who completes the return in the System.

Transfers

The Metrc System provides a complete and thorough transfer manifest process. All transfers must be initiated and received through the System. As inventory is moved from one licensee to another, the System tracks it to maintain the chain of custody.

Transfers must include packages from the original licensee's inventory. Licensees select the products and unit of measure that will be transferred from their current inventory; they also select a Transfer Type (e.g., Laboratory, Wholesale, Affiliated, etc.) from a predetermined list

Once required information is entered, the System automatically generates a transfer manifest containing the details about the transfer and the facilities involved (see Figure 10). The manifest is saved in the System and is printable and viewable in the System by both the shipping and the receiving establishment. Other information includes ship from name, license number and route description; destination address, name, license number, and address; and shipment product description, product ID, batch number, test results, quantity, and units of measure, including gross and net weights.



Destruction

Page 68 of 147



waste destruction. The State can maintain the Waste Method categories in the administration section of the System. The State can also receive notifications when waste is reported as destroyed.

3.2b: Tracking Number Assignment

The system must assign a tracking number to any cannabis that is to be dispensed to the patient or caregiver.

The Metrc System assigns a tracking number to any cannabis that is to be dispensed. The System generates a unique tracking number (receipt ID) for each dispensing transaction. Each sales transaction is recorded by package in the System using the unique identification number (Hex-ID) assigned to the package when it was tagged and inputted into the System. The time and date of sale as well as a unique receipt ID, price, license number, sales items, and quantities are captured and included in the details of the transaction. Transaction data also includes adjustments, such as for refunds, credits, and voids.

3.2c: Product Return to Manufacturer

Dispensaries will record information on all cannabis collected by the manufacturers. The system must allow dispensaries to record the following information for product returns:

- *The date of return;*
- *The identification number for patient or caregiver if patient or caregiver returns the product to dispensary;*
- *The number of marketing layers:*
- *The quantity of the cannabis in each marketing layer;*
- *The type of product;*
- *Testing batch number of cannabis collected; and*
- *Any other information required by the State*

The system must flag any inconsistencies or unreconciled record of returned or disposed cannabis product.

To record and track product returns, licensees create a sales receipt, entering the negative value for the returned product; the date of return; Patient or Caregiver Number; and the type, quantity of marketing layers, and cannabis quantity of the product. (Test results and batch number are forever tied to that product as metadata.) The System can flag any inconsistencies or unreconciled record of returned or disposed cannabis product via alerts or notifications. Alerts can be easily set up so that specific events, such as an unreconciled record, can automatically trigger a notification to the State.



3.2d: Dispensary Sales Record

The system must require dispensaries to maintain complete and accurate sales transaction records including:

- *The date of sale;*
- *The cannabis tracking number;*
- *The number of marketing layers;*
- *The amount of cannabis or cannabis product dispensed;*
- *The quantity of the cannabis in each marketing layer;*
- *The type of product;*
- *Testing batch number of cannabis sold;*
- *The identification number for patient or caregiver if purchase was done by a caregiver;*
- *The item number, product name, and description of items sold;*
- *The sale price; and*
- *Any other information required by the State*

The Metrc System maintains complete and accurate sales transaction records including all elements described in this requirement. The System generates a unique tracking number (receipt ID) for each dispensing transaction. Each sales transaction is recorded by package in the System using the unique identification number (Hex-ID) assigned to the package when it was tagged and inputted into the System. The time and date of sale, price, license number, order number, sales items, patient and/or caregiver information, weight or volume of product dispensed, and any other fields required by the State will be included in the details of the transaction. Transaction data also includes adjustments, such as for refunds, credits, and voids.

Sales transaction records can be reviewed via the System's sales reports. Other available sales reports include the following:

- Monthly sales reports
- Package sales reports
- Sales transactions reports

3.2e: Dispensary Inventory Reconciliation

The system must require dispensaries to reconcile all cannabis at the facility at the end of the business day against the sales and inventory tracking system. Inconsistencies will be flagged for the State personnel for investigation.

The Metrc System provides sales reports that include quantities and dollar amounts; dispensaries can use these to reconcile their sales. The State can also create custom notifications and/or SQL queries to investigate sales information. Furthermore, the System provides an open, secure, and web-based API (Application Programming Interface) for integration of external information systems, data, and hardware.

We have a well-established program for working with and validating third-party software providers (third-party vendors or TPVs) that integrate into the System's API and offer enterprise solutions to licensees. Over 500 software providers have integrated into Metrc, including point



of sale (POS), grow management, enterprise resource planning (ERP), laboratory inventory management (LIM), and other data systems.

POS integrators are able to perform daily sales/currency reconciliation using data from the System.

3.2f: Dispensary Label Issuance (Optional)

The system should issue a label with the following information:

- *The medical cannabis tracking number;*
- *The date and time the medication is being dispensed;*
- *The name and address of the dispensary;*
- *The patient's or caregiver's registry identification number;*
- *Any specific instruction for use based on manufacturer or department guidelines; and*
- *Any other information required by DOH*

As detailed in 3.1s, the Metrc System provides an open, secure, and web-based API (Application Programming Interface) for integration of external information systems, data, and hardware. That allows licensees and third-party vendors to integrate into Metrc to pull any required information in the creation of product labels.

We have a well-established program for working with and validating third-party software providers (third-party vendors or TPVs) that integrate into the System's API and offer enterprise solutions to licensees. Over 500 software providers have integrated into the Metrc System, including point of sale (POS), grow management, enterprise resource planning (ERP), laboratory inventory management (LIM), and other data systems. For example, Canix offers software and hardware (including product label printers) for licensees that integrate into the Metrc System.

Integrators and licensees alike are able to pull any tracked information from the System for use in printing on labels. If the State desires this information to be presented, saved, or accessed in a particular format specifically for the production of labels, Metrc will update the System to accommodate this need. We look forward to further discussing the approach, timeline, and specific requirements with the State.



IV.b.3. Tracking and Inventory Audit and Enforcement

3.3a: Vehicle Information

The establishments must be able to provide the following information to the department via this system regarding each vehicle that will be used to transport cannabis products:

- 1. Make, Model, and license plate number;*
 - 2. Proof of a valid insurance policy;*
 - 3. A description with photos of a locking compartment to be used to secure cannabis and cannabis products*
 - 4. Verification that the vehicle has a functioning alarm system; and*
 - 5. A description of how the cannabis and cannabis products will be maintained in a vehicle*
- Establishments can provide required information regarding each vehicle that will be used to transport cannabis products.*

Currently, the Metrc System captures the following required information: make, model, and license plate number; Employee ID; Driver's License No; Phone number; and the Driver's name. Metrc will update the System to accommodate additional State requirements on proof of valid insurance policy, a description with photos of a locking compartment, verification that the vehicle has a functioning alarm system, and a description of how the cannabis and cannabis products will be maintained in the vehicle. We are able to capture the additional features required and look forward to further discussing the approach, timeline, and specific requirements with the State.

3.3b: Internal Review

The system must provide the State personnel to review all establishment records as needed.

The System enables State personnel to review all establishment records. Metrc is first and foremost a regulatory compliance system. Built specifically for government oversight, the System provides the necessary visibility for adherence to and enforcement of rules, regulations, and statutes.

3.3c: Internal Dashboard

The system must provide a dashboard where the State personnel can review all flags of inconsistencies and irregularities in the cultivation, production, manufacturing, transporting, dispensing, and disposal of cannabis or plant material.

The System provides a dashboard that offers the State a quick reference point for aggregate data throughout the entirety of your program (Figure 11). The dashboard provides total numbers for licenses, users, plants, harvests, transfers, sales, patients, items, and strains with subsets within these totals as separate charts.

Each dashboard line graph can be selected to be expanded to show more detail, customize the displayed date ranges, or combine multiple data sets into one graph.

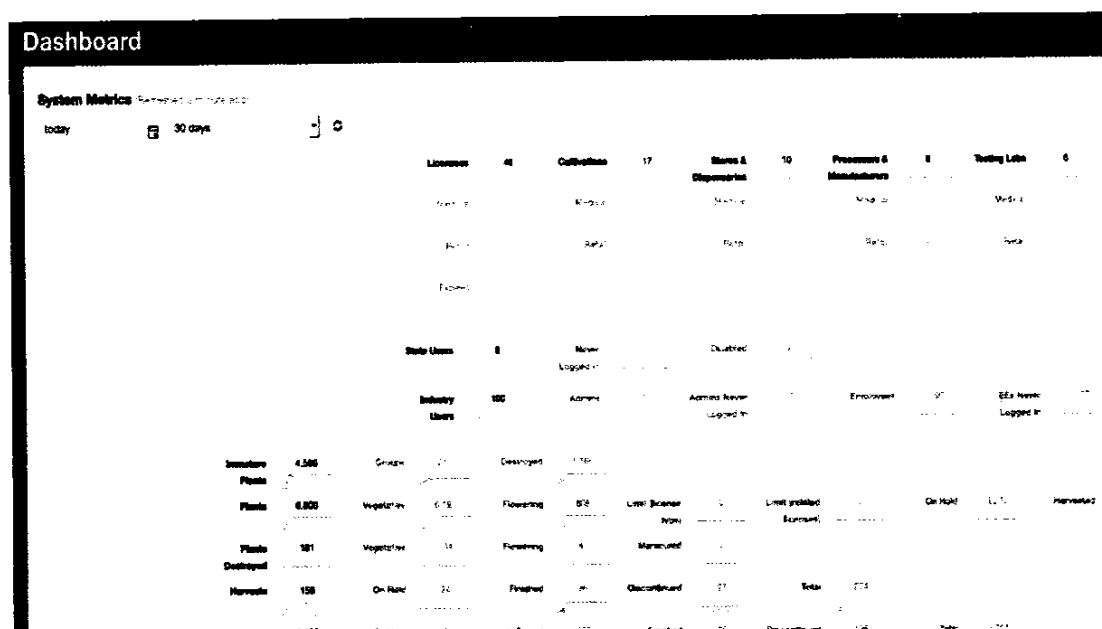


Figure 11. System Dashboard. *The State can use the dashboard as a quick reference for program data.*

3.3d: Tracking Reporting

The system must have reporting functionality with easy-to-use query function.

The system must have reporting tool with sort and filter function, an ability to save and share custom report specification, and an ability to export the report in various formatting including Microsoft Excel or PDF. The system should also come with template of reports including but not limited to the following:

- *Total number of internal flags by reasons;*
- *Breakdown of reasons for products that failed to meet testing standards;*
- *Price report by product type;*
- *Volume of sales by date range by individual establishment;*
- *Tax Collection Report by establishment ID;*
- *Breakdown of product purchased; and*
- *List of product and its price sold at individual establishment*

The Metrc System provides all of the tracking reporting capabilities the State requires. The System produces reports electronically, in a specified format (including CSV, PDF, MS Excel, and MS Word) and for a given timeframe. The System has over 80 pre-defined reports; plus, Metrc staff are available to create custom reports and queries for State users. Reports can be run on any information field in the System, including all of those listed in this requirement.

The System also includes an ad-hoc SQL Reporting Tool that allows State users to build custom queries on all data elements including metadata. Access to this tool is limited to State users with proper permissions. The results of these custom queries are available in standard industry formats such as PDF, MS Excel, MS Word, and CSV.



3.3e: Audit Logs

All actions by all users in the system should be tracked in an audit log including, but not limited to, username, action completed, and date/time stamp. When a user deletes information, the deletion is a "soft" delete and the data are not removed from the system and instead are still viewable to authorized personnel based on role- based security.

The Metrc System records all actions by all users in the system including username, action completed, date, and time. Furthermore, these events can be replayed at any point in history to reflect how the System looked at that point in time or can be used for data modifications or restoration. All System events are handled and processed as unique transactions that are subject to logging. These events are uniquely identified using plant and package serialization. In the event that users make a mistake, they are able to adjust (modify) the event and input the correct information. Such adjustments will also be recorded to retain an audit trail. These processes support licensees by persisting the event and then making the event available for oversight by the State.

The System provides a fully transparent audit trail of all cannabis supply chain events. The System tracks over 370 events throughout the supply chain, including production events like harvest date and yield in weight. The result of all events applied to an entity defines the entity's existing status. For example, an event tracked in the System can include details about the plant's growth and processing, such as harvest date and yield. Another event might be the creation of a 20-oz. package following harvest. If the package is then transferred to a dispensary, that event would also be tracked in the System. Should multiple sales events reduce the package to 0 oz., the System would list the package in the dispensary with 0 oz. of product left. Each event requires relevant data inputs, including product measurements (e.g., weight), reason, waste method, material mixed, and any additional notes (recorded via adjustments with reason codes assigned by the State). These events serve as a detailed audit trail and are viewable by the registrant in possession of the product as well as by the State or any regulatory user with appropriate permissions (e.g., Inspectors).

CASE STUDY 1 – AUDIT LOGGING SERVES REAL WORLD NEEDS

When the State of Colorado turned on the public API interface, they wanted to analyze active usage of the API and the level of success of third-party systems. They wanted details about how many times the public API endpoints were used; they also wanted to know the number of different actions performed when data was requested or modified. Our logging framework provided exact numbers of transactions and even the specific licensees using the public API interface. The level of detail available served the State well in obtaining early feedback and insight into the success of the public API deployment.



3.3f: Communication to Establishments

The system must provide an ability for the State personnel to set alerts and notifications. The system should provide automatic alerts or reminders based on system rules. Alerts may be set based on programmatic business rules, workflow process, or initiated by an authorized user. Alerts may be system-wide, program, or user specific.

Alerts can be easily set up so that specific events can automatically trigger a notification to the State. The System allows State users to create custom notifications via the System's rules engine. They are designed to help regulatory oversight by raising a flag and message when a violation occurs; however, they can be triggered by any number of conditions within the System. Each notification can be configured as minor to severe, and the message can be tailored accordingly. A minor notification might just log the notification, whereas a severe notification would immediately email or text a regulatory official and/or licensee.

3.3g: Data Integration

The system must have an ability to integrate with the following systems:

- 1. Cannabis Patient Registry;*
- 2. Cannabis Business Licensing System; and*
- 3. Point of Sale System*

The Metrc System has a robust Application Programming Interface (API) that will enable it to integrate with all three of the State's systems.

The Metrc System integrates with a variety of integrators' third-party data sources across the entire supply chain, including client-agency licensing systems and patient registries. For example, we have a positive and productive working relationship with NIC (Complia) and have successfully integrated with their patient registry solution in Maryland, Montana, Missouri, and West Virginia to validate patient or caregiver status and track purchasing limits. Other state system vendors we have integrated with include the following: Accela (CA, MI, and NV); Complia/NIC (MD, MO, OK, WV and MT); JD Software (MA); MyLo (CO); Sauper (ME); Custom Solution or Manual (AK, LA, OH and DC).



“Working with Metrc over the course of the last several years has been nothing short of an outstanding experience. Metrc’s industry-leading product has a robust set of APIs that makes integration a breeze. The Metrc team is world class and is always a pleasure to work with. We’ve integrated our cannabis patient registry and cannabis business licensing system with Metrc in several states, and each integration has been a tremendous success, creating a streamlined experience for regulators and industry stakeholders alike. I have no doubt Metrc’s platform will play a pivotal role in the success of South Dakota’s medical cannabis program.”

- Alex Valvassori, General Manager (Cannabis Licensing), Tyler Technologies (NIC Division)

We have also integrated with point-of-sale (POS) systems in all 16 jurisdictions we have partnered with. To date we have successfully integrated over 500 POS systems. The complete list is included as **Attachment 5**. Given our experience in 16 jurisdictions with vendors like NIC and many others, we are confident that our integration with the State’s systems, including the Cannabis Business Licensing System, will be achieved more quickly and reliably than any other track-and-trace vendor.

3.3h: Agent ID Login

Only the Cannabis Agent registered with the state can enter certain information in the system. The system should incorporate the integrated data from Cannabis Business Licensing System for log in to ensure that appropriate personnel at establishments are entering the information.

Metrc, in collaboration with the State, will create license types in the System. These different license types have certain configurable permissions that can be designated based on the type of business and the allowable actions within the State’s regulations. They can also set different tiers for each license type. These nuances can be used to align with the State’s unique licensing rules and third-party system (e.g., different tiers for different sizes of licensees).

If the State is licensing employees, it can create specific reportable profiles for industry licensed users. For example, common licensee user types include Owner, Administrator, Manager, Lab Sampler, Master Grower, etc. If the employees are not being licensed by the State, the State can designate Occupations. These occupations function similarly to designating a licensed Employee Type since they allow for designated roles to be identified by the licensed businesses. All of these Employee Types and Occupations allow for the State to report and identify the types of users within each licensed business based on its configuration decisions.



Users access the Metrc System via the Web Access layer, one of three layers in the System's infrastructure. All user types must use the W3C-compliant access layer to request secure authorization to use the System (Figure 12).

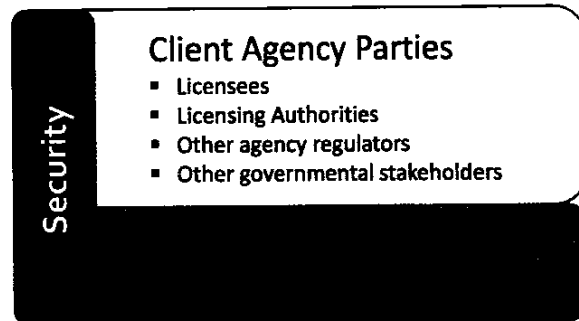


Figure 12. Access and Security. *User access to the Metrc System is provided by the Web Access layer.*

3.3i: Data Validation

The system must have data validation function to prevent missing data or data type errors.

The System validates data and prevents inconsistent data in a number of ways. The System prevents data type errors in online edits as well as data conditions that are logically inconsistent, such as entering future dates for completed activities. System operations are only available to the extent that they are consistent with past System activity—for instance, a facility cannot transfer a package if that package has already left the facility.

With some exceptions, the System does not prevent the entry of data that may not be factually accurate, even if such data entry reflects non-compliant behavior. This “non-forced compliance” approach to data entry is based on the guidance of regulators who want visibility into the actions of facilities. The approach does not prevent bad actors from knowingly misrepresenting their activities but does allow regulators to identify bad practices by facilities that are unknowingly non-compliant. Coupled with the ease of extracting data from Metrc via canned reports as well as ad-hoc queries, the System provides regulators with the tools they need to identify and follow up on non-compliant activity.

3.3j: Data Retention

Unless otherwise stated in Administrative Rules, all data in the system must be maintained for a minimum of 10 years.

The Metrc System maintains data for a minimum of 10 years per the State's Administrative Rules. The data is retained in the System's primary operational database, making it possible for users to continue accessing the data (subject to user role permissions and other functional restrictions) for that entire period.



IV.b.4. Security & Maintenance

3.4a: State Single Sign on

As part of the State's Identity and Access Management (IAM) strategy, the proposed system must integrate with the State of South Dakota's standard identity management service (SSO) which enables custom control of how citizens and/or state employees sign up, sign in, and manage their profiles. The SSO supports two industry standard protocols: OpenID Connect and OAuth 2.0. This identity management will handle password recovery. Multi-factor Authentication (MFA) is required for all application Administrators and may be required for other users. If the vendor is not able to fulfil this identity management standard, they will be considered disqualified and the proposal will not be evaluated.

The Metrc System will meet all the needs of the State's Identity and Access Management strategy, integrate with the State of South Dakota's SSO and deliver a robust authentication system that meets all the requirements listed. Single Sign On is currently road mapped to be built into the System and upon contract of work that effort will be prioritized and completed by the launch date. Multifactor Authentication is already built into the System, while with the State's SSO the MFA will be associated with the State's system authentication.

3.4b: Patient Identification Method

The system shall not identify any cardholder other than by the cardholder's identification number assigned by patient registry system.

The System meets this requirement as it has no mechanism with which to store cardholder information other than the identification number and associated start and end dates.

3.4c: Hosting and Data Access

The vendor must agree that the State will own the data tables and is able to manipulate data, run reports as needed, pull code tables, access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau and associated platforms. The State will give preference to vendors who can provide a cloud-based solution hosted/deployed onto the States' Microsoft Azure Cloud Tenant or a States preferred platform.

Metrc agrees that the State will own the data tables and is able to manipulate data, run reports as needed, and pull code tables. Metrc will work with the State to satisfy the need to access raw data and develop dashboards as needed through Microsoft Power BI, ESRI, Tableau, and associated platforms.

The production geolocation for the Metrc System, intended for this deployment, is the Azure North Central U.S. datacenter located in Illinois.



3.4d: Data Hosting Option

The vendor must host the solution, and the proposal must include the current server/system, specifications, software, and versions.

The Metrc System was created exclusively for government track and trace programs that support licensing and regulatory efforts. The Metrc enterprise solution includes Software as a Service (SaaS) deployed on a cloud-based Infrastructure as a Service (IaaS) along with service management and training and support for users and licensees.

Our infrastructure deployment is designed to be scalable both horizontally and vertically. This means that the System has the capability to increase capacity by upgrading system hardware and software. Consistent with industry-accepted best practices, our vertical scaling (e.g., scaling up) using the cloud allows us to use more, faster, or better hardware when needed. We are also able to scale horizontally (scaling out) by load balancing, using multiple machines to work as one machine.

Metrc is able to upgrade continually and transparently whenever the need arises, without impacting production service. We have added new servers, memory, processors, additional storage, and upgraded server operating systems throughout the System's lifespan. All of these upgrades and maintenance activities were completed successfully without unscheduled downtime by either hot-swapping components while the system was live or by performing work within approved scheduled maintenance windows.

We feel that these factors demonstrate that we have chosen the right cloud service provider for the Metrc System and that we have demonstrated a viable, reliable, and stable platform exists for the System.

The System utilizes the following:

- Servers: Azure Virtual Machines
- Operating System: Windows Server 2019
- Database: Azure SQL
- Firewalls: Azure Network Security Groups, windows firewalls and Azure Defender
- Networking: Azure networking services, Intrusion detection systems
- System software: Azure IaaS platform
- File Integrity Monitoring: Azure Defender
- Endpoint Detection and Response: CrowdStrike

Version information for discrete hardware is not available to those outside of Microsoft.



3.4e: Web-based Services

The system must have secure web-based access. The system must be accessible through various internet browser including Mozilla Firefox, Google Chrome, and Microsoft Edge. The system must also be mobile friendly.

The Metrc System's cloud-based architecture is accessible via browsers supporting a TLS 1.2 protocol, including Mozilla Firefox, Google Chrome, and Microsoft Edge. It is also mobile friendly and can be used via mobile devices, such as tablets and cellular phones that have internet access via a web browser. Users need not install or download software to use the System.

The System's SaaS environment is accessible through a secure, online login page. The System's Cloud-Based Access Layer allows user access through a secure web interface. All user types must use the W3C-compliant web access layer to request secure authorization to use the System.

Once logged in, licensees are presented with a user-friendly interface that displays only their information and allows them to easily enter product data. The fields and functionality of the System are configured to local laws and regulations, so it is clear what and when actions and information are required. And if a licensee is using enterprise software, like an inventory management or resource planning platform, they can integrate it into the System via our open API. This gives cannabis licensees the flexibility to choose enterprise software that suits their needs and to automatically push relevant data into the System to meet regulatory requirements.

3.4f: System Upgrades

The proposal must include system upgrade plan that includes but not limited to upgrade plan, types and frequency of upgrades. The purpose of this plan is to ensure that the proposed solution(s) have upgrade procedures that creates minimal impact or interference on system availability.

Metrc is able to upgrade the System continually and transparently whenever the need arises, without impacting production service. We have added new servers, memory, processors, additional storage, and upgraded server operating systems throughout Metrc's lifespan. All of these upgrades and maintenance activities were completed successfully without unscheduled downtime by either hot-swapping components while the System was live or by performing work within approved scheduled maintenance windows.

Metrc's change management process controls adjustments that are made to the Metrc solution. These changes can include, but are not limited to, such things as increasing the storage capacity of a server, publishing a new code fix to Metrc, or replacing a network firewall. The main attributes of our strategy for change management include:

- **Request for Changes** – Change Requests (CRs) are tracked in our Change Management System.



- **Defined approval process** – Major changes are assessed and approved by the Change Control Board (CCB). Minor changes are assessed for risk impact and approved by the Change Manager.
- **Changes of infrastructure** – Changes of infrastructure hosted at Rackspace are simultaneously run through their change management process in addition to ours.
- **System updates** – System updates are deployed through automation, which reduces the risk of errors being introduced due to manual human intervention.
- **Version control of source code** – Version control of source code allows code changes to be reviewed before they are moved into production which reduces the risk of errors being introduced.
- **Continuous integration process** – We employ a continuous integration process that makes sure automated builds of source code have unit, integration, and regression tests run before production acceptance.
- **Configuration data** – Our configuration data is stored in our change management database, which allows reviews and audits of changes introduced to the Metrc solution.
- **Separate environments** – We employ separate development, User Acceptance Testing (UAT), and production environments, which reduces the risk of errors being introduced to the production environment.

3.4g: System Issue Communication

The system must have an alert system where both external and internal users receive notification in case of system outage or issues with API in real time with estimated time needed for repair. The system must clearly communicate to all users when the issue is resolved.

Metrc has an assortment of methods for communication with both external and internal users. The Metrc System itself has a mechanism to allow for communication via banners, notification indicators, and automated emails depending on the event type. Metrc has personnel available to handle communication with both external and internal users in the event of an issue causing a system outage impacting the SaaS or the associated API. Any such event would go through an incident response procedure that includes communication when the issue is resolved.

3.4h: System Maintenance

The system must have a periodic maintenance to update the system, fix any known issues, and address requested improvements.

Metrc gives a high priority to routine preventive maintenance, and we replace hardware on a rolling cycle as a preventive measure. Although the Metrc System is provided to the State as a SaaS solution, the performance of routine maintenance on System components is also a key component of the service we provide.

We are often able to perform routine maintenance while the System is online. Examples include the regular backup of databases and operating system images, the application of non-



system critical patches that do not require a system reboot, disk management, SAN storage allocation, etc. We agree to perform non-routine maintenance, such as a feature updates or anything requiring downtime, within the scheduled downtime maintenance windows approved by the State and provide the required notifications whenever possible.

Metrc periodically deploys releases throughout the year based on the number of changes being pushed out and timing requirements for legislative directives. Updates are deployed through automation, which reduces the risk of errors being introduced due to manual human intervention.

3.4i: Data Security

The data security for the proposed solution (s) must meet the requirements set by the State and HIPAA.

The Metrc System's data security meets State and HIPAA requirements.

We recognize that the System, its components, and the data that drives it are essential not only to stakeholders but also to public health and safety. Given that, we maintain strict data privacy policies and procedures to meet the State's business objectives and regularly review and update them to comply with the latest industry best practices (NIST, SANS, and SOC 2 Trust Service Criteria). We also comply with federal security standards for security categorization (FIPS 199), with special focus on confidentiality of data and protection of proprietary software/data, and controls for developing a secure and resilient information system (NIST 800-53).

Metrc maintains policies to meet the necessary business objectives. These policies are regularly and periodically reviewed and updated to comply with the latest industry best practices. The policies and updates are made available and communicated to personnel, along with support for interpreting and understanding them as necessary. These policies are supported by a set of implementation standards and guidelines, both of which enable us to enforce and validate them through periodic reviews, audits, and updates.

Our policies begin with comprehensive risk assessment strategies, which include senior management oversight. Risk assessment strategies focus on identifying administrative roles and responsibilities which apply, not only to Metrc personnel, but also to vendors and contractors. We also conduct risk assessments to update our policies to align with security requirements, including the following.

- Federal Privacy Act of 1974 (Privacy Provisions)
- PCI-DSS and its Cloud Computing Guidelines

In addition to our privacy policies and enforcement, all public websites contain a Privacy Policy Statement and a Notice of Collection where applicable. These are easily accessible and visible on the front (or entry) page of the System and our public website.

Practices for protecting data at rest are defined and controlled in accordance with the State's information classification policy requirements for sensitive data. Encryption, tokenization, and



masking/obfuscation are examples of technologies used on organizational electronic devices and media which store information. The encryption strength of the keys and algorithms employed is proportional to the assurance-level requirements of the devices and storage media.

Encryption keys are protected and managed for data recovery, misconfigurations, and forensic investigations in accordance with data at rest protection practices. Data at rest protection practices are periodically audited, reviewed, tested, and updated. As an example, SQL Server databases will make use of certificates of 4096-bits key lengths (the maximum currently supported for encryption), and alternatively, 3456-bits key lengths where 4096-bits are unsupported, such as by the Transparent Data Encryption (TDE).

Additionally, data is backed up in accordance with the SLAs. The backup service for the primary datacenter is designed to back up the database and virtual machines (VMs) on a regular schedule at a specified time. Full database backups are performed weekly and differential backups are completed on all other days. Transactions are backed up every 30 minutes. Backups are encrypted and stored in the production data center. Data is replicated via log shipping to the disaster recovery location in the continental United States. All backups are stored offsite for two weeks.

3.4j: User Role Permissions

User Roles must limit CRUD (Create, Read, Update, Delete) access per Role. Addition of new Roles and changes to Role CRUD access must be easy.

The Metrc System has the ability to provide all functionality described in this requirement. The System is a highly configurable, robust platform that was built specifically to help regulators track and trace cannabis products from seed to sale. As such, it is designed to be adaptive so that changes can be made quickly and easily as rules and regulations evolve over time. User roles will limit CRUD (Create, Read, Update, Delete) access per role. The State will also find it easy to add and modify roles. The System's configurability includes features that do not require any additional System development and can be configured either directly by the State's administrator or by Metrc personnel at the State's request.

Define User Roles and Access

Metrc, in collaboration with the State, will create license types in the Metrc System. These different license types have certain configurable permissions that can be designated based on the type of business and the allowable actions within the State's regulations. They can also set different tiers for each license type. These nuances can be used to align with the State's unique licensing rules and third-party system (e.g., different tiers for different sizes of licensees).

If the State is licensing employees, it can create specific reportable profiles for industry licensed users. For example, common licensee user types include Owner, Administrator, Manager, Lab Sampler, Master Grower, etc. If the employees are not being licensed by the State, the State can designate Occupations. These Occupations function similarly to designating a licensed



Employee Type since they allow for designated roles to be identified by the licensed businesses. All of these Employee Types and Occupations allow the State to report and identify the types of users within each licensed business based on its configuration decisions.

Users access the Metrc System via the Web Access layer, one of three layers in the System's infrastructure. All user types must use the W3C-compliant access layer to request secure authorization to use the System (Figure 13).

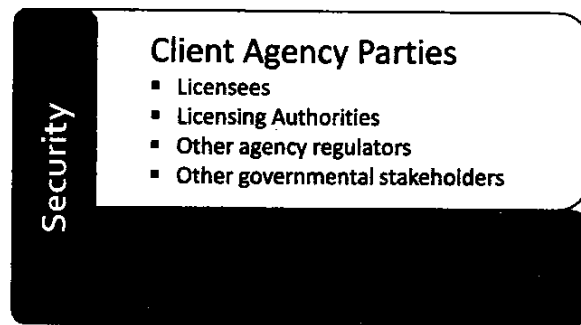


Figure 13. Access and Security. *User access to the Metrc System is provided by the Web Access layer.*

Create and Update New Roles

The State and licensees will have complete role-based permissions. Administrators create and maintain new and existing users and define permissions based on user type or individually expressed permissions. In addition, the administrator or authorized user may choose to add individual roles and/or read-only access to other areas within their purview. Licensee administrators can create specific user access for their users with corresponding permissions.

The State administrator can define and adjust user roles, which will, in turn, have granular permissions assigned. User roles can be easily interpreted as a set of permissions grouped under a single name, which in this context is the user role's name. State-defined user roles will be available to be assigned to any State users created within the Metrc System.

The aggregated set of permissions from the assigned role will be applicable to the user, thereby granting the user access to the areas where the applicable permissions are accepted, and restricting access where not permitted. Defined user roles can be adjusted at any time by the State. Role changes will be immediately effective to all users assigned to the role. Role-based security functionality makes user authorization easier for administrators to manage.

3.4k: Data Encryption

The system must utilize data encryption when data is sent.

Practices for protecting data at rest are defined and controlled in accordance with the State's information classification policy requirements for sensitive data. Encryption, tokenization, and



masking/obfuscation are examples of technologies used on organizational electronic devices and media which store information. The encryption strength of the keys and algorithms employed is proportional to the assurance-level requirements of the devices and storage media.

Encryption keys are protected and managed for data recovery, misconfigurations, and forensic investigations in accordance with data at rest protection practices. Data at rest protection practices are periodically audited, reviewed, tested, and updated. As an example, SQL Server databases will make use of certificates of 4096-bits key lengths (the maximum currently supported for encryption), and alternatively, 3456-bits key lengths where 4096-bits are unsupported, such as by the Transparent Data Encryption (TDE).

The System uses data encryption when data is sent via enforced TLS 1.2. Data loss protection (DLP) is a security concept to detect and prevent all channels through which critical and confidential information can be leaked. The focus of DLP is to prevent data leaking from within the Metrc organization and from the Metrc internal infrastructure. For example, DLP would be used to detect that a Metrc employee has emailed sensitive data to someone outside the organization. Since Metrc is a public-facing web application, we can only control data within our control. Data that is legitimately extracted from Metrc is outside the scope of this section; however, Metrc does employ security best practices for the client-side browser.

We use operational controls and privacy enhancing technologies to limit data leakage. These include fields identifying all confidential data, encryption, firewalls, authorized use system access controls, and system audit logs. In accordance with NIST SP 800-122, we implement a DLP solution that monitors network communications and prevents sensitive personal identifiable information (PII) from leaving our networks. In addition to these technical controls, we use administrative policies such as acceptable use policies, confidential data policies, and email policies, as well as providing privacy training, to further safeguard information privacy and control access to Metrc data.

Metrc data is classified under one of several categories: in-transit, in-use, and at-rest, which are defined as follows.

- **In-transit Data** – Data that needs to be protected when in transit including HTTP/S, S/FTP/S, SMTP.
- **In-use Data** – Data that resides on end-user workstations that need to be protected from being leaked through removable media devices like USBs, DVDs, and CDs.
- **At-rest Data** – Data that resides on local storage media or server storage.

3.4l: Sensitive Data Storing

The system must not store authentication credentials or sensitive data in its code.

The Metrc System does not store authentication credentials or sensitive data in its code base for production systems. The static code analysis that is performed against the System's first-



party code detects such flaws in the event that this type of data were to be included in our code either mistakenly or maliciously.

3.4m: Interfaces

The vendor must describe how the system can adapt to business necessary interfaces using widely adopted open APIs and standards. Additionally, the State expects that the vendor will make available/expose software services and publish documentation for those software services that would enable third party developers to interface other business applications. A detailed description of system capability shall be included in the Proposal.

The Metrc System has a robust Application Programming Interface (API) that provides all required capabilities. It includes an out-of-the-box RESTful JSON interface to receive external data (i.e., license and patient information) into the System. The quickest and most efficient manner of transmitting data is through this RESTful API. Data transmitted through this interface receives immediate format and data validity feedback from the System.

Integration with external sources, including Enterprise Resource Planning (ERP) systems, is controlled by Web Services. The Metrc System's web services are created using C#, HTML5, RESTful methodology, and JSON and contain the following parts:

Regulatory API: Exposes the Regulatory reporting functionality via secure API.

Industry: Exposes the industry application functionality via secure API to allow third-party solution providers to report cannabis activity on behalf of licensees. These third-party integrators can work with Metrc to become validated on the Metrc Industry API.

Licensing: This is a service that supports generic RESTful integration with regulatory licensing solutions.

Licensees can input data directly into the System or integrate their enterprise software into the System. This gives them the flexibility to choose any ancillary software that suits their needs and automatically push relevant data in real time into the System via the API to meet regulatory requirements.



"Cova strives to help retailers stay compliant in their operations, and our integrations with Metrc's API serve a key role in this. Because much of their compliance information is kept in sync between systems, they can keep everything up to date easily. We've seen this integration significantly improve the accuracy of data reported to regulators.

Due to the complexity of keeping our system integrated with Metrc across many different markets, their documentation and support have been critical to our success. When we have issues or questions, their API support team is always very quick to respond. This helps us to make fewer assumptions about how the system should behave, improving the level of compliance."

- Dave Emmett, Product Owner, Cova Software

The State can integrate external systems, such as licensing and patient registry, with the System via our open API and pull specified data for various purposes, including reports and analysis. The System can also send reports to an external system, such as an FTP site—some client states use this functionality to help validate tax returns.

3.4n: Data Normalization

The system will have the ability of data normalization to reduce and eliminate data redundancy.

The Metrc System operates on a relational database platform. The System takes full advantage of this using standard industry normalization approaches: operational tables have unique system-assigned IDs, and those IDs are used in other tables to reference specific records. This data model minimizes redundancy, which allows for accurate updates and efficient storage.

Key database entities also support functional keys, which allows both online users and API clients to uniquely identify what records they are working with. Plants and packages are uniquely identified by the Hex-IDs associated with their tags. Third-party integrators who work with multiple licensees use the license number to identify which licensee each transaction relates to. The licensing API similarly uses the license number as a key.

3.4o: Design Pattern

The system permissions will follow an "explicitly granted" design pattern.

All user types must use the W3C-compliant access layer to request secure authorization to use the System. The System has a complete role-based permissions system. Administrators can



define permissions based on user type or individually expressed permissions. In addition, the administrator or authorized user (regulatory or licensees) may choose to add individual roles and/or read-only access to other areas.

3.4p: Environment

The system will require close/separate environments for: development, testing and production.

We employ separate Development, User Acceptance Testing (UAT), Sandbox, and Production Environment, which reduces the risk of errors being introduced to the Production Environment.

Metrc will deploy the following environments to support the State's implementation:

- **Development Environment** – This environment is used only by Metrc developers.
- **Testing Environment** – This environment is used to train State users on the System and is where the System configurations are set and tested before they are transferred to the production environment before go-live. After go-live, this environment continues to be used to test out potential configuration changes as well as new System functionality prior to release to production.
- **Sandbox Environment** – This environment is maintained to match production and is used to provide third-party integrators (TPI) the ability to test and validate their systems through the API. TPIs are given access on request and are required to pass a validation process in the sandbox environment before they are provided with a production environment API key.
- **Production Environment** – This environment is used by licensee users to record all actions taken with cannabis within their operations and by State users to track and trace all cannabis plants and product in South Dakota. This environment is configured based on State regulations and is maintained to the most current version of the Metrc System platform.

3.4q: Session Timeouts

The system will enforce session timeouts during periods of inactivity.

The System employs security best practices for client-side browsers, including server-side session timeouts.

3.4r: Credential Storing

The system will not store authentication credentials or sensitive data in its code.

The Metrc System does not store authentication credentials or sensitive data in its code base for production systems. The static code analysis that is performed against the Metrc System first-party code detects such flaws in the event that this type of data were to be included in our code either mistakenly or maliciously.



3.4s: Change Management Documentation

The system will utilize change management documentation and procedures.

Metrc's change management process controls adjustments that are made to the Metrc System. These changes can include, but are not limited to, such things as increasing the storage capacity of a server, publishing a new code fix to the System, or replacing a network firewall. The main attributes of our strategy for change management include:

- **Request for changes** – Change Requests (CRs) are tracked in our Change Management System.
- **Defined approval process** – Major changes are assessed and approved by the Change Control Board (CCB). Minor changes are assessed for risk impact and approved by the Change Manager.
- **Changes of infrastructure** – Changes of infrastructure are simultaneously run through their change management process in addition to ours.
- **System updates** – Metrc updates are deployed through automation, which reduces the risk of errors being introduced due to manual human intervention.
- **Release notes** – We share notes on upcoming releases once deployed to the testing environment to ensure communication of new features before they are deployed to the production environment.
- **Version control of source code** – Version control of source code allows code changes to be reviewed before they are moved into production, which reduces the risk of errors being introduced.
- **Continuous integration process** – We employ a continuous integration process that makes sure automated builds of source code have unit, integration, and regression tests run before production acceptance.
- **Configuration data** – Our configuration data is stored in our change management database, which allows reviews and audits of changes introduced to the Metrc System.
- **Separate environments** – We employ separate Development, User Acceptance Testing (UAT), and production environments, which reduces the risk of errors being introduced to the production environment.



3.4t: Customer Support

The vendor must provide technical and end-user support via phone and email between 7:00 AM and 9:00 PM CT, 7 days per week. Additionally, the vendor must be available and has ability to respond to critical issues in timely fashion regardless of the time of the incident. The detail of disaster recovery and support requirements are outlined in the Appendix C, Section 9.2 (page 32).

Extensive Support Options & Availability

Metrc's support program is designed to ensure that every System user gets an answer to their issue, quickly and personally. Call-in, email, and web-based support is unlimited and designed to address immediate and ongoing needs.

Metrc provides a fully staffed and dedicated Support Desk, reachable via a local toll-free telephone number and/or email. State and licensee users will also have access to a support portal that provides a self-service center (with chatbot assistance), a Q&A knowledge base, and a live chat option (Figure 14).



Figure 14. Zendesk Chatbot. Live chat gives State and licensee users get easy, online help when they need it.

The Support Desk operates Monday through Friday from 7:00 AM CT to 9:00 PM CT, seven days a week. Voicemails and emails can be left/sent outside those hours and will be addressed at the next regularly scheduled operating time. Support Desk schedules can be adjusted to support the State's requirements.

State users will have direct access to an assigned contract manager and our senior leadership. This ensures that the State has access to multiple senior-level employees for emergency support, even after hours. The State can also contact our senior leadership for any inquiry, whether about track-and-trace or a regulatory topic. And should the State seek insight or perspective from any of our 16 regulatory clients, we will facilitate an introduction.

Moreover, Metrc has amassed a team of industry experts and is happy to offer complimentary advisory services to the State and other stakeholder agencies as part of our engagement. We



routinely engage with regulators, legislators, and industry organizations regarding the use and implementation of cannabis rules and regulations. Metrc will offer the State best practices and information regarding the steps or approaches being taken by other cannabis regulatory bodies and will offer guidance based on that information to improve the performance of the State's System and program. These services are completely optional and may be used at the State's discretion at no additional charge.

Support Access, Quick Resolution

We provide unlimited call-in and email support to address immediate and/or ongoing needs, ensuring everyone using the System gets an answer to their issue quickly and personally. After many years of supporting cannabis oversight and the industry, we have identified areas where system users frequently need our assistance, enabling our support team to quickly address the most common inquiries. **Our average wait time for answer to a phone inquiry is under five minutes, and our first-contact resolution is over 95%.**

Our support team is focused intently on providing quality outcomes. This outcome-based approach empowers our support team members to take the time necessary to ensure effective use of the System, which leads to more accurate and actionable data in the System. It also leads to more satisfied users and more confidence in using the System.

Support Team Expertise

Helmed by a director with 25 years of combined customer service, marketing, and training experience, our team of 75+ support professionals and 9 supervisors provide the State and licensee users with a full suite of resources. Metrc support team members are all full-time, U.S.-based Metrc employees. We do not employ third-party support staff.

Metrc's Customer Support department is comprised of various teams, each with a different specialization. We assign support tickets by specific areas of expertise to ensure that system users benefit from each team's cumulative and extensive knowledge. When a System user calls or emails, it is not uncommon for them to connect with a team member who has multiple years of experience in numerous jurisdictions in their area of expertise. Our specialized teams include the following:

- **The Credentialing Team** is usually the first point of contact licensees have with the Support Desk. These team members provide an invaluable service to regulators by confirming that a business is properly licensed, the appropriate business owners have access to the Metrc System, and all training requirements are met. Licensee users benefit from having their first use of the System guided by a support desk member who specializes in getting business accounts in the System properly activated and set up for use. The Credentialing Team walks users through the initial steps of setting up their account and can typically offer a 48-hour turnaround for all credentialing requests Monday through Friday. In addition to the initial onboarding services, the Credentialing Team provides services when offboarding licensees is necessary (e.g., when a licensed company sells its business to another entity, if allowed). At such times, Metrc can



support the transition process by, for example, changing the primary Metrc System administrator and/or transferring data and product from one business to another.

- **The Reports Team** is a dedicated team of experts focused on standard System-generated reports. They help educate System users about specific reports and how to run them. They also help identify solutions for the data needs of licensees. They are experienced at efficiently and comprehensively addressing complex scenarios.
- **The Investigations Team** is expressly used by regulatory agencies. An Investigations Team member can walk investigators through the inspection process, answer questions, and assist with actual investigations. This team is especially useful in the early stages of Metrc System usage, helping regulators get up and running quickly by teaching them how to effectively apply System data to their monitoring, compliance, and enforcement activities.
- **The Reconciliation Team** provides guidelines from the regulator to help licensees cleanup their Metrc System accounts. Members of the Reconciliation Team answer questions for licensees and work with the regulators' investigators to make sure cleanup is performed within the jurisdiction's guidelines. This valued service helps licensees and investigators efficiently update Metrc System records. It is not uncommon for regulators to find non-compliant use of the System during routine and complaint-based inspections. After such findings, it is everyone's goal to get the cannabis products to a compliant state. In these cases, licensees may call Metrc support and use the Reconciliation Team's expertise to get inventories entered properly into the System.
- **The Testing (Laboratory) Team** is dedicated to the testing practices of each jurisdiction where the System is deployed. This team provides problem-solving support regarding the laboratory testing required for each regulatory framework. Team members provide walkthroughs on how to use the System to report details about the testing processes performed, and they help correct mistakes. They work closely with the regulators to understand the testing requirements and ensure that errors are corrected in a manner that aligns with the State's regulations. The Testing Team is extremely talented in researching complex issues and offering guidance about reconciling errors.
- **The API Team** supports third-party integrators (TPIs) that are currently validated (or would like to become validated) by Metrc to use the System's robust and open API. TPI support includes answering questions about the validation process, problem-solving API use, and helping to resolve any other API issues the integrator may encounter.
- **The Billing Team** supports licensees by helping with expedited tag orders and industry-reporting fees. The Billing Team can help licensees complete orders, make payments, and produce receipts, and can answer all questions regarding tags, tag orders, or industry-reporting fees.
- **The Outreach Team** reaches out to licensees to build and maintain exceptional working relationships, all while continuously gathering feedback to further fine-tune and streamline the System's overall support processes. In addition, this team can provide State-initiated outreach to licensees on special projects and plans.



- **The .CSV (Comma-Separated Values) File Extension Team** assists smaller, licensed businesses that do not work with outside vendors to integrate with the System. For these smaller businesses, Metrc offers many ways to use the System with ease and provides CSV import functions for various areas of the software. CSV team members are experts on each format that can be used to import files into the System and use their expertise to assist with troubleshooting and resolving errors. The CSV Team works closely with these valued small businesses and builds strong and successful working relationships.
- **The System Issues Team** is one of our most specialized teams. This dedicated team of specialists is critical for logging and tracking all reported system issues and ensuring that all reported issues follow the requirements outlined in the Expected Process for Incident Reporting and Severity Table. Once a licensee or regulatory agency user reports a System issue via phone or email, it is immediately assigned to the System Issues Team, which analyzes the issue and starts the escalation process. First, communication with the regulatory agency user/licensee is established and the incident details are confirmed/verified. A Systems Issue Team supervisor will then alert the program manager and escalate the issue to the Technology department. The issue is constantly tracked, and all tickets related to this incident for that client are cross-linked in the tracker for comprehensive reporting to the regulatory authority. Once the issue is resolved, all users are contacted and informed of the resolution. This team is known for its rapid response in handling reported issues with ease and professionalism.

Access to Software Engineering & Technical Resources

Each specialized team (described above) includes Level One through Level Three Specialists. Support specialists are assigned to specific levels of customer support inquiries. Our Level Three Support team consists of members of both our engineering development and business management teams. They provide State users with quick resolution, feedback, troubleshooting, and support for complex issues. These individuals are experts in their fields and are responsible for assisting Level One and Level Two personnel daily, as well as researching and developing solutions to complex issues identified by State users.

Whether during or outside normal operating hours, the support team acts as a liaison between users and the technical engineering staff. The support team acknowledges receipt of all requests, per agreed-upon Service Level Agreement (SLA) requirements, and forwards the request to the relevant engineering team, preventing internal duplication of efforts and ensuring that a team member promptly formulates a response.

Metrc also maintains a team of full-time technical and engineering staff at our Lakeland, Florida offices. At any time during non-office hours, at least one technical and engineering team member is on call. The team's knowledge is diversified, and, while some specialize in hardware and others in software, all team members understand the entirety of the Metrc System and are familiar with the most widely used W3C-compliant browsers.



Incident/Problem Logging

To manage log ticketing, the Metrc support team relies on Zendesk, an online cloud-based customer service software that provides all the smart automations necessary for our team to get things done quickly and efficiently. It also gives State and licensee users access to a support portal that offers a self-service center (with chatbot assistance), a Q&A knowledge base, and a live chat option. Each phone call, email, and voicemail automatically generates a ticket for the appropriate team member to resolve. These tickets allow us to keep track of issues, questions, and requests and then effectively track and relate that information back to State as needed. All support calls and emails are logged to capture issues and trends.

Issues are assigned a severity level—critical, high, medium, or low—and are resolved as expeditiously as possible, per agreed-upon standards. The Support Desk has a specific escalation process. Each support person is trained on the process and how to escalate potential issues quickly and efficiently to ensure timely resolution.

The Support Desk's problem management responses are measured through data collected in Zendesk and MiTel's MiCloud Connect Contact Center and are reported using Microsoft Excel. Incidents are viewable and accessible to the State. Moreover, each month we can provide the State with reports that give an overview of the type of issues and questions the licensees have sent to support (email and phone). Our reports also include a complete breakdown of the data, displaying percentages of each support type, which helps the Metrc program management contact and the State's contact, working in tandem, to determine if additional communication is needed through bulletins to address ongoing industry concerns.

3.4u: Support and Maintenance Plan

The proposal must include system update plan. The plan at minimum must include the following items:

- 1. Testing: Provide the testing plan that describes a plan for user acceptance training, development of user acceptance testing environment, stress regression, and performance test plan.*
- 2. Implementation: Provide the implementation plan of the application that describes how the implementation is prioritized, planned, managed, and executed.*
- 3. Ongoing Maintenance: Provide maintenance plan that describe level of support service provided with estimated response time.*
- 4. Modification: Provide methodologies for how modifications are charged to the State.*

The following addresses key elements of our System Update Plan including testing, implementation, ongoing maintenance, and modification.

1. Testing

Provide the testing plan that describes a plan for user acceptance training, development of user acceptance testing environment, stress regression, and performance test plan.

Metrc's testing process includes a strategy phase, goal definition, analysis of test coverage, and a plan to implement automation, as described in the following paragraphs.



Strategy Phase: Test Plan Formulation

Metrc developed and uses a Master Test Plan that serves as a unifying model for all other test plans. We follow the ISO/IEC/IEEE (29148:2018) standard for software test documentation. This process ensures that we can test the System and updates from end to end to demonstrate that what we create does what it is supposed to do.

Our test strategy encompasses functional (dynamic) and non-functional (static) testing, load capability testing, regression testing, and security testing.

Goal Definition – Functional and Static Testing

Functional testing includes black-box testing and white-box testing. Black-box testing is performed by the test lead who verifies that the software components meet the predefined requirements by feeding them input (positive and negative) and examining the output. The purpose of black-box testing is to examine the software's functionality without drilling down to its internal structure or workings. The purpose of white-box testing is to test the internal structure or workings of an application, as opposed to its functionality. This is performed by the developers and the user experience designer.

Static testing includes a static code review and is performed by the developer lead. The purpose of the source code review is to highlight possible issues within static (non-running) source code by using techniques such as taint analysis and data flow analysis.

Analysis of Test Coverage and Plan to Implement Automation – Testing within the Agile Framework

Metrc's System Test Plan defines the structure used to test each specific software product to ensure it meets the requirements that guided its design, is sufficiently usable, and can be installed and run in the intended environments. These plans include unit test plans, system-specific user acceptance test plans, and security test plans. The test lead designs a suite of user acceptance tests of the System's functionality. The functionality is tested with circumstances expected to pass and circumstances expected to fail.

Unit Test Plan: Metrc's Unit Test Plan sets out the procedure by which we test the individual units of source code and/or program modules with associated control data.

User Acceptance Test (UAT) Plan: The UAT Plan defines the procedures by which we test the user acceptance criteria, the load capability, and any regression testing required. Quality Assurance analysts perform the UAT, load capability testing, and any regression testing. They also write and perform the prescribed testing. The System generates a report detailing the list of tests performed and their pass/fail status.

Security Test Plan: The Security Test Plan defines the test methods we employ to ensure that the product is secure. We perform security testing by using the Veracode Static Analysis platform to verify that the System protects data and maintains functionality as intended. We test the System to ensure that confidentiality, availability, authorization, integrity, authentication, and non-repudiation are maintained. Our developers use the Veracode Static



Analysis platform testing to generate results that are prioritized based on severity for remediation. Our developers also use Veracode's Web Application Security platform to test the System for architectural weaknesses and vulnerabilities in running web applications, then provides validation or items for remediation.

2. Implementation Plan

Provide the implementation plan of the application that describes how the implementation is prioritized, planned, managed, and executed.

The following pages provide an overview of Metrc's implementation process as well as a sample, high-level project schedule that meets the State's desired six-month implementation timeframe.

Implementation Plan

Metrc's Implementation Plan is a comprehensive plan that includes details about the following: Metrc System, implementation process, fit/gap analysis, communication, time management, scope management, issue management, risk management, system configuration, State administrator configurable items, quality assurance, metrics, testing, and third-party integrators.

The following provides an overview of Metrc's five-phase implementation process.

Phase 1: Predecessors and Planning (Project Kick-Off Meetings)

Initiation, Discovery, Fit/Gap Analysis

Kick-Off Meeting and Initial Working Sessions
 Preliminary Project Plan and Specification
 New State Page on Metrc.com
 Preliminary Requirements to Engineering
 Testing Environment Access Sites and Training

Project Schedule

Project Implementation Plan to include:

- Disaster Recovery Plan
- System Configuration
- Fit/Gap Analysis
- Communication
- Time Management
- Scope Management
- Issue Management
- Risk Management
- State Administrator Configurable Items
- Quality Assurance
- Metrics
- Testing



Initial State and Industry Training

- Third-Party Integrators

Phase 2: Inputs and Processes (Project Charter and Project Plan)

Project Charter and Project Plan

Engineering Site, Test and Production

Credentialing Process for Support

Terms and Conditions

RFID Tag Provisioning, Testing, Configuration

Mobile Device Configuration and Testing

Additional Documents:

- Initial State User Manual and Guide
- API Specification
- Guide for Testing Labs
- Initial Supplement for Industry

Phase 3: Outputs (Requirements Analysis, Development, and Testing)

Requirements Analysis, Development, and Testing

Roadshow Plan, Industry Roll Out Planning, Industry Training Plan

Initial State Training

Integration Testing

User Acceptance Testing (UAT)

Metrc Final Review

Additional Documents:

- Final State Manual
- State Handheld Manual
- Final Industry Manual
- Final Industry Supplement

Phase 4: Go Live (Training, Deployment, and Implementation)

Training, Deployment, and Implementation

Update Schedule

Update and Train Support Team

Configuration of Support Ticketing System

Final Gap Analysis and Business Requirements Review

Update Project Plan and Specification Documents

Go-Live State Training Updates



Training, Deployment, and Implementation

Lab Training

Push from Testing to Production Go-Live

Phase 5: Successors (Reporting and Ongoing Delivery of Service)

Reports and Ongoing Delivery of Service

Final Documentation:

- Close Out Report
- First Quarterly Operations Report
- Maintenance and Operations Report

Advanced Training

Operating concurrently with all five phases are ongoing activities that support on-time delivery and continuous improvement. These include:

- Weekly status reports
- Ongoing documentation updates
- Requirements tracking and validation
- Future-state feature planning
- Stakeholder engagement, approval, and escalation
- User training and support

Project Schedule

The following is a sample, high-level project schedule. We are providing it to give the State a sense of our well-planned approach to projects. We understand that the Project Schedule is subject to approval from the State.

Sample Project Schedule			
Project Stages	Deliverables	Target Start Date	Target Due Date
Predecessors & Planning	• Kick-Off Meeting	12/1/2021	2/9/2022
	• Initial Project Plan and Specification		
	• Customization Delta --> Final Requirements to Engineering		
	• New Program Webpage --> Opening Statement and FAQs		
	• Sandbox Access Sites --> Training, API/Integration		
	• Deliverable Documents --> Project Schedule, Data Dictionary, Disaster		



Project Stage			
	Recovery Plan, Configuration, Gap Analysis		
Inputs & Processes Prototyping	<ul style="list-style-type: none"> Engineering Site, Test & Production -> Provision, Testing, Configuration Mobile Device Configuration & Testing RFID Tag Provisioning Third-Party Vendor (TPV) API User Agreement Deliverable Documents -> Initial State User Manual & Guide, API Specification, Guide for Labs, Initial Supplement for Industry 	2/9/2022	3/17/2022
Outputs Testing	<ul style="list-style-type: none"> Industry Roll Out Planning -> Road Show Plan, Industry Training Plan Initial State Training Integration Testing User Acceptance Testing (UAT) -> UAT Test Plan Metrc Final Review Deliverable Documents -> Final State Manual, State Handheld Manual, Final Industry Manual, Final Industry Supplement 	1/28/2022	3/31/2022
Go-Live Implementation	<ul style="list-style-type: none"> Update & Train Support Team Support Ticketing System Configured Final Gap Analysis & Business Requirements Review Update Project Plan & Specification Documents Go-Live State Training Updates Lab Training Push from Testing to Production Go-Live 	3/31/2022	4/14/2022
Successors	Final Documentation -> Close-out Report, Performance Report, Maintenance & Operations Plan	4/21/2022	4/30/2022
On-Going			
Delivery of Service	Advanced Training		



3. Ongoing Maintenance

Provide maintenance plan that describe level of support service provided with estimated response time.

The following describes the ongoing maintenance Metrc provides after implementation and provides details about our Service Level Agreements. For details about Metrc's support program, please see our response to 3.4t above.

Ongoing Maintenance

Metrc's maintenance and support services are designed to deliver reasonable, consistent, high-quality support for Metrc customers for the duration of our contracts.

After implementation, Metrc transitions to the Maintenance and Operation (M&O) plan. During M&O, we work with the State to address ongoing items and perform System updates deemed beneficial for the State's business needs. Because communication is important, we continue to visit project stakeholders during M&O. We also identify targeted site visits or in-person trainings that might benefit the State. This process of engagement allows Metrc to be prepared for client requests, so subsequent implementations can be well thought out, speedy, and efficient.

Metrc gives high priority to preventive maintenance, which we perform to avoid application problems and component failures. And, while the System is provided to the State as a SaaS solution, the performance of routine maintenance on System components is also a key component of the service we provide.

Some of the System's components allow us to perform routine maintenance while the System is online. Examples include the regular backup of databases and operating system images; the application of non-system critical patches that do not require a system reboot; disk management; SAN storage allocation, etc. We perform non-routine maintenance, such as a feature updates or anything requiring downtime, within scheduled downtime maintenance windows approved by the State. Metrc replaces hardware on a rolling two-year cycle as a preventive measure.

Standard Service Level Agreements

Below are Metrc's standard Service Level Agreements (SLAs); if necessary, Metrc is willing to further explain and discuss these with the State. Metrc has two primary types of SLAs: System and Support. Our System SLA focuses on the Metrc System's availability and operation, while our Support SLA focuses on our support team's availability and responsiveness to user inquiries. Each is described in further detail below.

System SLA

Constant monitoring of system use allows our team to respond immediately to any issues. Metrc's engineering staff use a variety of monitoring programs and tools to continually assess the system's security, use, and performance (see Figure 15). We track hypervisors, load balancers, virtual machines (VMs), firewalls, and all system-related hardware and software



performance. We monitor server traffic, server traffic errors, hardware performance failures, and automated data hits (indicating possible hacking attempts), to name a few.

Tool Name	Purpose	What it Provides	Importance to the State
Quest Spotlight for SQL Server	Monitor SQL Server performance	Provides detailed performance statistics of database servers	Allows Metrc to react to performance demands at the database level. Metrc engineers can also react to events such as resource contention and long-running queries that may be over-utilizing the System.
New Relic	Capture System availability status	Captures the external availability of the System	Allows Metrc and the State to see current availability status and collected raw data.
	Monitor internal component	Captures real-time performance data of each server that is part of the System, and captures drive utilization	Allows Metrc to react to changing performance demands and to predict future capacity needs.
Microsoft Excel 2010	SLA Management and Reporting	Reporting SLA objective status	Allows Metrc to report the status of SLA management to the State.

Figure 15. Monitoring System Performance. Monitoring and management tools support SLA management.

The State can access reporting information via on-line automated tools or may choose to receive periodic status reports (monthly, quarterly, etc.). We track performance statistics as part of our continual monitoring and will make this information available upon request.

The following are Metrc's standard SLAs, but we will adjust during negotiation to meet the State's contractual requirements, should Metrc be selected.

Metrc's Standard System SLAs	
Redundancy	A test environment configured identically to the production environment that will remain operational throughout the term of the contract and any extensions to be used by the State for testing and training.
Sustainability	99.95% guaranteed network uptime.
Database	Database failover.
Site Back-up	Site failover and replication.
Server Back-up	Server failover.



Minimum Standard System SLAs	
Name of SLA	Description
Downtime	One-day recovery time objective (24 hours max downtime).
Monitoring	24/7 database and application availability monitoring.
Notifications	In the event of an alert, notification of the issue and response shall be promptly provided to the State.
Recovery	30-minute recovery point objective.
Data Back-up	Full backups weekly and incremental backups daily for non-database data.
Full Back-up	Full database backups nightly.
Differential Back-up	Differential database backups every 4 hours.
Data Logs	Database transaction logs every 30 minutes.
Disaster Recovery	Use of SQL Server Log Shipping to send the data to the remote site. Data will be automatically loaded into the disaster recovery database. Two running copies of the database will run full time at both sites. The disaster recovery site will be 30 minutes behind at most. The backups will be stored in Texas and Illinois.
Dependencies	Identification of all server and application service dependencies, including ports and protocols (in a format approved by the State).
Software Versioning	List of all software versions and updates at the time of transition.
Hypervisor Tool	Hypervisor tool for migrating VMs from the hosting environment to the State infrastructure will be VMware compatible.
Hosting	Hosting Services shall support secure socket layer (SSL) communication over the internet.

Levels of Severity and Incident Resolution for System SLAs					
Severity Level	Title	Description	Initial Response	Incident Categorization	Incident Resolution
1	Critical	Production system is halted and/or data has been corrupted. If there is no reasonable work-around available, a patch may be produced. When an acceptable resolution is provided, the incident shall be downgraded to a lower priority.	15 mins - 45 mins	1 hour	Resolution or workaround available in 4 hours or less. Incident may then be closed, and problem opened to evaluate.



Incident Response					
Level	Priority	Incident Description	Resolution Time	Escalation Time	Resolution Process
2	High	Incidents render a feature inoperable without a resolution or workaround. They do not cause the production system to be inoperative, but they disrupt the normal business operations.	30 mins - 2 hours	2 hours	Resolution or workaround available in 8 hours or less. Incident may then be closed, and problem opened to evaluate.
3	Medium	Incidents render a feature inoperable with acceptable work around to be used on an interim basis until incident addressed with a more effective work around and/or fix.	1 hour - 4 hours	12 hours	Incident resolved in 24 hours or less. If the incident cannot be resolved in 24 hours, it leads to a problem. The incident is closed, and a problem is opened to evaluate further.
4	Low	Incidents have little impact on the business and application including questions not answered in the vendor documentation and documentation errors. Incidents may be addressed in a future release.	1 hour - 8 hours	24 hours	Incident resolved in accordance with agreed-upon timeframes. If the incident cannot be resolved with a bug fix or patch in the next release, it leads to a problem. The incident is closed, and a problem is opened to evaluate further.

Support SLA

METRC's Standard Support SLA		
SLA Name	Description	Objective
Support Services – Calls Missed Percentage	Number of calls not answered and serviced by the Support Desk divided by the total of all Support Desk calls. Calls answered by voicemail will be considered answered.	≤ 10%



Service Name	Description	Metric
Support Services – Wait Time	The average time a call is placed on hold, waiting to speak with a customer service representative.	≤ 5 minutes
Support Services – Service Time	Average time elapsed from when a user first speaks to a Help Desk resource until the user service is provided, and the user disconnects. If the call is escalated to Tier 2 or Tier 3, the time that the call is escalated will represent the service end time for this SLA. The ticketing system's automatic notification feature will prevent callbacks and repeat calls for the same problem.	≤ 10 minutes
Support Services – Resolution Percentage	Percentage of all Help Desk calls resolved during the first call divided by the total of all Help Desk calls. Escalation to Tier 2 or 3 will constitute resolution being provided during first call in the context of this SLA. The ticketing system's automatic notification feature will prevent callbacks and repeat calls for the same problem.	≥ 95%
Correction of Deficiencies Critical Level – Time to Respond	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc representative acknowledges initial notification.	< 60 minutes
Correction of Deficiencies Critical Level – Time to Correct	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc maintenance personnel correct the Deficiency.	< 12 hours
Correction of Deficiencies Moderate Level – Time to Respond	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc representative acknowledges initial notification	< 24 hours



Correction of Deficiencies Moderate Level – Time to Correct	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc maintenance personnel correct the Deficiency < 7 calendar days
Correction of Deficiencies Minimal Level – Time to Respond	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc representative acknowledges initial notification < 24 hours
Correction of Deficiencies Minimal Level – Time to Correct	Time difference between the time the State or Metrc (whichever is earlier) reports and records the problem or outage in the problem tracking tool and the time Metrc maintenance personnel correct the Deficiency < 30 calendar days

4. Modifications

Provide methodologies for how modifications are charged to the State.

Metrc is mindful of the dynamic nature of implementing cannabis policy and expects that the legal framework governing its sale will continue to evolve significantly for the foreseeable future. Our business model, pricing structure, and the adaptability of our system enable us to include the development, testing, and implementation of reasonable system enhancements at no additional cost.

In the jurisdictions we serve, Metrc has implemented more than 450 System changes and enhancements at no additional cost to our client agencies. This is especially significant given the pace of change to rules, regulations, and statutes in legal cannabis markets and the fact that many software providers consider change fees standard practice.

While we work with our regulatory clients to avoid change orders whenever possible, change orders are sometimes necessary. In 2019 and 2020, five of our sixteen client agencies requested changes that were mutually determined to be outside the scope of our contractual agreement. Three of those agencies requested the addition of more data storage for product photos, while the other two requested significant software enhancements.

We place our customers' needs at the forefront so that changing requirements can be easily incorporated into the system. It is important to note that the other eleven client agencies that did not require change requests are more reflective of our model. Metrc is available to provide



additional context and information on our pricing model and historical change requests if requested by the State.

3.4v: Point of Sale (POS)

The system must be able to integrate with point of sale system via an Application Program Interface (API) to ensure all data required by the State is recorded in system. The system must accept all major credit cards as well as payment via cash or check. The proposal must include the list of all POS systems that the system has successfully integrated.

If a licensee is using third-party software like an inventory management or point of sale (POS) platform, they can integrate it into the Metrc System via our open API. This gives cannabis licensees the flexibility to choose third-party software and hardware, such as barcode scanners for patient and/or caregiver cards, that suits their needs and to automatically push relevant data into the System to meet regulatory requirements. We also allow for patient and/or caregiver information to be manually entered into the System through our user interface in case licensees do not use third-party software or hardware.

Metrc accepts all major credit cards as well as check or money order.

Metrc has successfully integrated with over 500 integrators, of which over 390 provide point of sale (POS) services. This includes vendors like Flowhub, Cova, Greenbits, Growflow, and Yobi. For the State's ease of reference, a full list of our POS integrators is included in **Attachment 5**.

3.4w: Integration Plan

Integration plan, timeline, and previous integration experiences with the list of vendors/system must be submitted for the following system:

- *Patient registry, verification, and business licensing system and*
- *External Point of Sale system(s).*

Patient Registry Integrations

Metrc has successfully integrated with six different state system vendors across our 16 client jurisdictions. The full list is provided in section 3.3g on page 75.

Our experience with patient registries covers several types of business needs from simple validation ("is patient valid?") to tracking purchased quantities and limits ("is the patient within their allotted purchase amount?"). Patient validation implementations utilize two different methods: 1) the patient registry pushes limited unidentifiable patient information to Metrc, or 2) Metrc communicates with the patient registry using a Metrc-specific formatted JSON message to validate patients. Our preferred approach is the first of these options, hosting the limited unidentifiable patient information in Metrc, so that the Metrc System is self-contained and can continue functioning even during maintenance periods.



The second most used patient registry integration is tied to patient purchase limits. This configuration tracks purchases by patient numbers and, optionally, presents a message to dispensaries when purchases go beyond the limit. For the industry side, this helps ensure that patients get their allotted amounts with very little effort. And on the regulator side, this functionality helps monitor patients and dispensaries not following the regulation or legislature.

Integration work typically begins in the “Predecessor/Planning” stage of implementation when we work to jointly define what integrations are needed, continues in the “Inputs & Processes Prototyping” as integrations are designed and built, and concludes in the “Outputs Testing” stage with integration testing and UAT. During the “Inputs & Processes Prototyping” phase, Metrc works with State or vendor personnel to define specifics about the approach.

Business Licensing Systems

Metrc also integrates with business licensing management solutions. These integrations consist of one-way API calls, meaning that the state systems provide information about business licenses by sending JSON-based information through the Metrc API. (The System also provides the ability to upload information via CSV as a backup.) The System uses the information sent by the state systems to apply State-configured rules based on license types.

Like integrations with patient systems, licensing integration work typically begins in the “Predecessor/Planning” stage of implementation with sandbox setup, continues in the “Inputs & Processes Prototyping” with the documentation of API specifications, and concludes in the “Outputs Testing” stage with integration testing and UAT. During the “Inputs & Processes Prototyping” phase, Metrc provides State or vendor personnel with details about the expected inputs to the API, including information about how new records are differentiated from updates and how the data will be utilized and displayed in the System. This allows the state system team to better identify what data they should be extracting from the state system to send to Metrc. Our straightforward integration approach and availability to support the State means that the data exchange can usually be implemented in a very short timeframe.

Our testing and UAT environments fully support integration with state systems, allowing us to work with the state system team during the “Outputs Testing” phase to test the API calls so the State can have confidence in the efficacy of the integration.

Interoperability with External Systems

While the System tracks cannabis products through the entire supply chain, some of our licensees desire other software solutions (e.g., grow management, point of sale, enterprise resource planning, and/or compliance functionality) to meet their specific needs. Metrc allows validated, independent software providers to integrate with our System to minimize duplication of data and facilitate data links. This enables the industry to track additional information related to their products and automate processes in a way that works best for their business. Metrc integrates with over 500 third-party industry-serving software providers, over 390 of which provide point-of-sale (POS) services.



Metrc hosts a Sandbox Environment that is maintained to match production and is used to provide third-party integrators the ability to test and validate their systems through the API. Metrc also has a support team dedicated to validating third-party integrators and addressing their questions and inquiries.

For third-party integrators to be validated to use Metrc's API, they must first demonstrate a basic understanding of how the API works. Metrc's API support team provides would-be integrators with access to documentation as well as access to the Sandbox Environment, where the integrator can work with test data to refine their understanding and test out their integration code. The integrator identifies what specific areas of Metrc they want to integrate with, choosing from Plants, Harvests, Packages, Labs, Sales, and administrative functions, and what States they want to work with. Once the integrator has demonstrated their understanding of the API calls that relate to their selected areas of the System, Metrc provides them with an integrator API key to the appropriate production environments. The integrator's customer (the licensee) then provides them with the licensee's own user API key; the two keys in conjunction allow the integrator to perform tasks on the licensee's behalf.

Typically, there will be a large influx of third-party integrations immediately following go-live as licensees begin using the System. However, we continue to offer this integration support through the entirety of the contract, since integrators may change over time. Integrators who are already interacting with the System in other states can typically be validated in short order. Because of these factors, the timeframe for a vendor to start integrating with the System varies and doesn't fit neatly into the implementation stages for any given state.

3.4x: Unique Identification Tag/Labels

The system must utilize a readable smart-chip technology including Radio Frequency Identification or RFID, or comparable technology to track cannabis plants and product. The smart chip technology should contain the following information:

- *Plant tag unique identification number*
- *Plant grow address*
- *Plant Owner License Identification Number*
- *Tag issue date*
- *Any other information required by the State*

The System uses RFID chip, a barcode, and a human-readable unique number identifier (Hex-ID) to track marijuana through every phase of the supply chain in real time.

RFID, Barcode, and Unique Identifier

Like every track-and-trace system, the Metrc System has both a digital and a physical component: software and tags. The software is used to input and store data and acts as a centralized database of every single marijuana plant and product in the legal market, including relevant information such as location, quantity, origin, and test results. The tags uniquely identify plants and tie the physical plants and products to the information in the software. Our proprietary tags are centrally produced by Metrc and contain licensee information, a scannable



barcode, a human-readable number, and an RFID chip embedded with a globally unique, non-repeating identification number known as a Hex-ID.

Tag provisioning starts with a licensee placing an order for RFID tags. Once tags are ordered, a printing process begins. The physical tags start as a blank roll of tags loaded onto a machine that prints licensee information, a barcode, and encodes an RFID chip embedded in each tag with a unique Hex-ID.

The Hex-ID is assigned to the specific licensee during the assignment process and is used to track and record chain of custody events within the System. As tags are printed, the globally unique identifier is generated, encoded on the embedded RFID chip, displayed as a barcode on the surface of the tag, and recorded in the Metrc System (Figure 16). In addition to Hex-ID, the tag is tied to the plant grow address, plant owner license identification number, tag issue date, and any other information required by the State.



Figure 16. Unique Identifier Assignment Process. *The Metrc Hex-ID unique identifier is assigned to and made known to a specific licensee through the provisioning process.*

During the tag printing, each tag's tag ID (TID) value is read and recorded in the database. The TID is a read-only unique identifier that is etched into the tag's chip during manufacturing. This number prevents any attempt to counterfeit the tag. When a tag is verified for authenticity, the TID is compared to that recorded in the database. Later, when the tag is in the field, the TID and Hex-ID can be used for factor identification to detect fraud.

The barcode application standard used by Metrc is UCC 128 compliant. The RFID tag is ISO/IEC 18000 Part 6 compliant. Both of these are open standards that are commercially available off-the-shelf technologies. This approach creates visual consistency for the State and can reduce costs by eliminating the need for licensees to purchase the equipment and materials required to apply identification information to plants or packages. It also provides the State with secure and verifiable information in the tag, which is used to automate compliance.

Metrc's tag provisioning process eliminates labor-intensive data mapping and number matching—a weakness in other approaches. Our process eliminates compliance issues and regulatory processes that would be required to monitor for proper tag creation were licensees to perform these functions themselves. The Metrc methodology thereby provides a strong chain of custody that is clean and supports a regulatory foundation with integrity, since it is built upon accurate, verified data.



“...because Metrc provides unique tag numbers for plants and packages, license holders looking to break the law have a much more difficult time diverting or inverting product than they would with other systems that let users create their own tag numbers. This strengthens the industry and makes cooperation with governing bodies all the easier. To increase transparency, users should never be able to produce their own non-unique tag numbers.”

- Kyle Sherman, President Flowhub Inc., a leading solution provider to the Cannabis Industry

3.4y: Unique ID Printer/Plant ID Printer

The proposed solution must offer a unique identification code printing capability to streamline the inventory and chain of custody record keeping for Cannabis Establishment Employees and the State personnel.

The System offers a unique identification code printing capability to streamline the inventory and chain of custody record keeping for the State and licensees. Please see our response to 3.4x above for details.

3.4z: Plant ID Reader

The proposed solution must offer a barcode scanning capability for unique identification to be used by Cannabis Establishment Employees and the State personnel.

Every plant and product accounted for in the Metrc System is traceable to a patented Metrc-engineered radio-frequency identification (RFID) tag. While every tag is equipped with RFID, the tag also has a scannable barcode and human readable component. But there are distinct advantages to the State with the System’s RFID functionality.

Barcode and other QR code-scanning systems rely on an inspector having manual line-of-sight contact with each tagged plant and product. An inspector using an RFID handheld can collect data on multiple plants and products simultaneously. In large licensee operations with thousands of plants and tags in a given location, field agents using RFID readers can complete site inspections in hours instead of days—and with greater accuracy.

Audits and inspections are designed to ensure that plants and products within the legalized markets are not diverted for illicit sale. The search feature on the RFID handheld device enables investigators to quickly locate missing or misplaced plants and packages. In an evaluation of capability based on internal tests, one inspector using an RFID reader can accomplish in hours what would take four inspectors an entire day to achieve using barcode, QR code, or any other optical line-of-sight scanning technology.



“Studies conducted at the University of Florida’s Center for Food Distribution and Retailing report that a cultivation inspector is six to eight times more efficient using a RFID handheld reader than a barcode scanner. Metrc’s RFID readers have a read range of more than ten feet and do not rely on line-of-sight, giving them a scan rate that is twenty times faster than barcode scanning. In field tests conducted at licensee facilities in Colorado, ALR-H460 RFID readers were able to scan more than 600 plants in ten to fourteen minutes.”

If awarded this contract, Metrc will provide two Spector Handheld RFID devices to the State at no charge to support its field audits and investigations.

Each Spector device provided by Metrc includes the following, at no additional fee:

- Pre-installed, fully configured software (Investigator App) that has already been tested so the unit is ready to use right out of the box.
- Seamless integration with the Metrc System.
- Software and device training and support, including documentation for all client users.
- Replacement of damaged units or parts, as covered by warranty.
- Repair of damaged units or parts, as covered by warranty.
- Replacement of outdated devices and software (additional detail below).

The RFID handhelds enable the State’s staff to scan cannabis inventory quickly and efficiently, then compare it to what is reported in the System. Instead of barcode readers, which require that every tag be manually scanned, RFID readers enable all tags to be automatically and passively read. When considering that licensees potentially have thousands of plants and tags at a given location, the RFID readers can save field agents hours of time in a single visit and helps ensure that no tag is mistakenly missed.

RFID readers have a read range of more than 10 feet, have a scan rate faster than a barcode, and do not rely on “line-of-sight” to read tags. In field tests conducted at licensee facilities in Colorado, readers scanned more than 600 plants in 10-14 minutes. The search feature also enables investigators to quickly locate missing or mis-located plants or packages. In a total evaluation of capability based on our internal tests, one inspector using RFID can accomplish in hours what would take four inspectors an entire day to achieve using barcode, QR codes, or any other optical line-of-sight scanning technology.

Metrc will update the Investigator app (the readers’ software) on an ongoing basis, to improve or expand functionality. The updates will be available for the current and previous version of the app.



As each new generation of the Spector handheld reader is released, Metrc releases a new version of our Investigator app to comply with the new hardware specifications. Unfortunately, the new software versions may not work on previous generations of devices. Because of that, Metrc will upgrade the device and software to the latest generation available for both, starting when the Investigator app is two versions behind. This ongoing replacement comes at no additional cost and is the primary benefit of the leasing model.

IV.b.5. Operation

3.5a: Previous Government Experience

The vendor must provide a minimum of 2 example of a successful software implementation of a system similar to this RFP and 3 references from governmental agencies.

Metrc contracts with regulatory agencies in 16 U.S. jurisdictions: Alaska, California, Colorado, Louisiana, Maine, Maryland, Massachusetts, Michigan, Missouri, Montana, Oklahoma, Nevada, Ohio, Oregon, West Virginia, and the District of Columbia for their cannabis track-and-trace systems. Eight of these jurisdictions use the Metrc System to monitor their medical marijuana markets, and the other eight use it to monitor both their medical and adult-use markets.

Our performance in 16 different jurisdictions, has earned us the reputation as the most trusted and experienced provider of cannabis traceability ("track-and-trace" or "seed-to-sale") solutions in the United States. We are the only track-and-trace provider with a **100% renewal rate** in our government contracts, as well as the only track-and-trace provider to successfully replace an incumbent vendor, as we did in both Nevada and Maine.

Metrc has never had a service/contract terminated, expired, or not renewed in the last three years.

Successful Software Implementations and References

The following tables provide details about five successful software implementations and include all details required in RFP section 4.4.

Information	Reference #1
Company name	Colorado Department of Revenue, Marijuana Enforcement Division
Contact person	Kyle Lambert
Title	Deputy Director
Address	1697 Cole Boulevard, #200
City	Denver
State	Colorado, 80401
Telephone number	303-205-2355
Email address	Kyle.Lambert@state.co.us
Size of account	\$1.6 million for initial project
Contract period	Initial contract signed November 2011; current contract extends through 2026



Brief summary of services	<p>Project Description: Metrc, working with the Colorado Department of Revenue, Marijuana Enforcement Division, created and deployed the first-ever state marijuana track and trace software solution (contract start in 2011 and Go-Live in 2013). Today, Metrc tracks both the medical and recreational (adult-use) marijuana markets, on behalf of the State of Colorado, utilizing RFID unique identifiers integrated inside the Metrc software. Metrc was awarded the first contract in 2011 and continues to deliver services via contract extensions.</p> <p>Other Pertinent Information: Metrc was custom-built to meet Colorado's rules and regulations leading up to the historic launch of the first adult-use cannabis market in the United States on January 1st, 2014. In a July 2014 Brookings Institute report, "Colorado's Rollout of Legal Marijuana is Succeeding," the author refers to the Metrc System as the "backbone of the Colorado regulatory system." We partnered closely with the regulators from the beginning of marijuana legalization to ensure the Metrc System empowered the Colorado MED to meet all the state-specific statutes and regulations.</p> <p>As part of the implementation in Colorado, Metrc trained over 90% of the licensees in the state of Colorado in under 90 days. During the initial 60-day implementation period, we successfully provisioned over 1,000,000 plant and package RFID tags. A recent audit of the use of data by Colorado's Marijuana Enforcement Division found Metrc to be the "cornerstone of the State's regulatory structure."</p>
---------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Company name	Montana Department of Public Health and Human Services
Contact person	Erin Ducharme
Title	Bureau Chief
Address	2827 Airport Road, PO Box 4210
City	Helena
State	Montana, 59620-4210
Telephone number	406-444-7877
Email address	educharme@mt.gov
Size of account	\$796,000 for initial project
Contract period	Initial contract signed April 2018; current contract extends through 2022
Brief summary of services	<p>Project Description: In Montana, medical cannabis was legalized at the ballot in 2016 and later became subject to a more robust regulatory framework following legislation that was passed in 2017. Metrc provides our seed-to-sale system, working closely with NIC that provides its platform supporting business licensing, employee credentialing, and patient/caregiver registration.</p> <p>Other Pertinent Information: The licensing system in Montana went</p>



	<p>through significant legislative changes in 2020 and most recently the spring of 2021; these changes altered the business structures and self-provider or home grow rules for patients and caregivers. As the licensing system has been revised, the information updates are being sent to the Metrc System via the API. Even with these changes, our System is able to consume the most current information in the latest format. In this market, since NIC and Metrc are integrated providers, the licensing system data for individuals (patients/caregivers/employees) and businesses retain the chain of custody and source of truth in an end-to-end regulatory solution in real time.</p> <p>Furthermore, the State recently expanded its contract with Metrc to support its adult-use market. (Metrc previously provided our solution to the state's medical market.) Metrc is currently working with the State on the expanded implementation.</p>
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Information	Reference #3
Company name	Nevada Department of Taxation Compliance Division
Contact person	Tyler Klimas
Title	Director
Address	1550 College Parkway
City	Carson City
State	Nevada, 89706
Telephone number	702-486-0606
Email address	tklimas@ccb.nv.gov
Size of account	\$384,000 for initial project
Contract period	Initial contract signed December 2017; current contract extends through 2022
Brief summary of services	<p>Project Description: In addition to providing the State's marijuana seed-to-sale software solution, we provide third-party integrator support (POS systems), software solutions, cloud hosting, and technical updates. We also provide regulator and licensee training and support. Training is offered via webinars, YouTube videos, user guides, and manuals. Support includes industry bulletins and a support team available via email and telephone. We also provide an experienced team of subject-matter experts with multi-state support experience.</p> <p>Other Pertinent Information: The Nevada Department of Taxation initially awarded the contract to MJ Freeway in 2016. Metrc took over the contract in July 2017.</p> <p>The State of Nevada discontinued their Seed-to-Sale contract with MJ Freeway and given the exigent circumstances, this deployment was completed in under 60 days for over five hundred active licenses to gain access and begin reporting into the System. The</p>



	project covers seed-to-sale system implementation and management for both Medical and adult-use Marijuana for the state of Nevada.
--	------------------------------------------------------------------------------------------------------------------------------------

Information	Reference ID
Company name	Maine Office of Marijuana Policy (OMP)
Contact person	Erik Gunderson
Title	Director of OMP
Address	162 State House Station
City	Augusta
State	Maine, 04333-0162
Telephone number	207-287-3282
Email address	Erik.Gundersen@maine.gov
Size of account	\$540,000 for initial project
Contract period	Initial contract signed February 2020; current contract extends through 2026
Brief summary of services	<p>Project Description: The Metrc System is the adult-use and medical seed-to-sale tracking system for the regulation of legalized marijuana marketplace, including the ability to track patients purchases against the control limits and to record any adverse reactions to the medicine (product), including RFID Unique Identifiers integrated inside the Metrc System.</p> <p>Other Pertinent Information: The Maine Office of Marijuana Policy contract was initially awarded to BioTrack in 2019. Metrc took over in February 2020 to rapidly onboard both the adult-use and medical markets due to a mutual contract termination between the State and BioTrack. Metrc was able to fully implement the System and begin accepting industry users in 30 days.</p>

Information	Reference ID
Company name	Oklahoma State Department of Health, Office of Management and Enterprise Services (OMMA)
Contact person	Dr. Kelly Williams
Title	Director of OMMA
Address	1000 NE 10th St
City	Oklahoma City
State	Oklahoma, 73117-1299
Telephone number	405-388-4804
Email address	Kelly.Williams@health.ok.gov
Size of account	\$540,000 for initial project
Contract period	Initial contract signed August 2020; current contract extends through 2030



Brief summary of services	<p>Project Description: In addition to providing the State's marijuana seed-to-sale software solution, we provide third-party integrator support (POS systems), software solutions, cloud hosting, and technical updates. We also provide regulator and licensee training and support. Training is offered via webinars, YouTube videos, user guides, and manuals. Support includes industry bulletins and a support team available via email and telephone. We also provide an experienced team of subject-matter experts with multi-state support experience.</p> <p>Other Pertinent Information: The low costs for market entry and high demand in the State led to explosive growth of the State's market. That, combined with the procurement and implementation of Metrc two years into the program, meant that Metrc was tasked with training and credentialing a record number of licensee users in record time. Between March and April, Metrc trained an average of 500 licensee users per day.</p>
---------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Contact Information

The following table includes the contact information for our remaining 11 client agencies. We encourage the State to contact each state agency to evaluate Metrc's performance on our contracts.

Client Contact List	Contract Start/End
Oregon Liquor Control Commission T.J. Sheehy, Director of Analytics & Research 503-873-5000 Tj.sheehy@oregon.gov	2014 - Present
Alaska Alcohol & Marijuana control Office Glen Klinkhart, Director 907-269-0350 Glen.klinkhart@alaska.gov	2016 - Present
Maryland Medical Cannabis Commission Lori Dodson, Deputy Director 410-487-8065 Lori.dodson1@maryland.gov	2016 - Present
Michigan Department of Licensing and Regulatory Affairs, Marihuana Regulatory Agency Andrew Brisbo, Executive Director 517-284-8590 Brisboa@michigan.gov	2017 - Present
Ohio Department of Commerce, Medical Marijuana Control Program Greg Mcilvaine, Senior Policy Advisor 614-728-8352 Gregory.mcilvaine@com.state.oh.us	2016 - Present
Massachusetts Cannabis Control Commission	2018 - Present



Shawn Collins, Executive Director 617-701-8400 Cannabiscommission@state.ma.u	
District of Columbia, Department of Health Arian Gibson, Enforcement Officer 202-442-9069 Arian.gibson@dc.gov	2017 - Present
California Department of Food & Agriculture, Bureau of Cannabis Control Chris Cox, Project Director 916-274-6372 Chris.fox@cdfa.ca.gov	2017 - Present
Louisiana Department of Agriculture & Forestry Tabitha Irvin, Director Medical Marijuana Program 225-922-1244 Tgray@ldaf.state.la.us	2018 - Present
Missouri Department of Health and Senior Services, Division of Licensure & Regulation/Medical Marijuana Program Amy Moore, Deputy Director 573-751-6234 Amy.moore@health.mo.gov	2019 - Present
West Virginia Department of Health and Human Resources, Bureau for Public Health, Office of Medical Cannabis Jason R. Frame, Director 304-356-4124 Jason.r.frame@wv.gov	2020 - Present

3.5b: Legislative Updates

The vendor must provide legislative and regulatory updates within the scope of the proposed 5-year bid/contract at no expense to the State.

Metrc is mindful of the dynamic nature of implementing cannabis policy and expects that the legal framework governing its sale will continue to evolve significantly for the foreseeable future. Our business model and pricing structure and the System's adaptability enable us to include the development, testing, and implementation of reasonable system enhancements at no additional cost.

In the jurisdictions we serve, Metrc has implemented more than 450 system changes and enhancements **at no additional cost** to our client agencies. This is especially significant given the pace of change to rules, regulations, and statutes in legal cannabis markets and the fact that many software providers consider change fees standard practice.



3.5c: Risk Management and Communication Plan

The vendor must provide a written risk management and communication plan for the proposed 5-year term of the contract.

Metrc will provide written Risk Management and Communication plans for the proposed five-year team of the contract. The following describes our approach to each.

Risk and Issue Management

Metrc's Risk Management process follows the guidance provided by the National Institute of Standards and Technology (NIST) "Guide for Conducting Risk Assessments" to monitor, manage, and mitigate risk. As Figure 17 illustrates and the following paragraphs describe risk management, covers risk monitoring, assessment, and response. Each of these areas is influenced by—and, in turn, influences—the unique risk framework that is adopted by an organization.

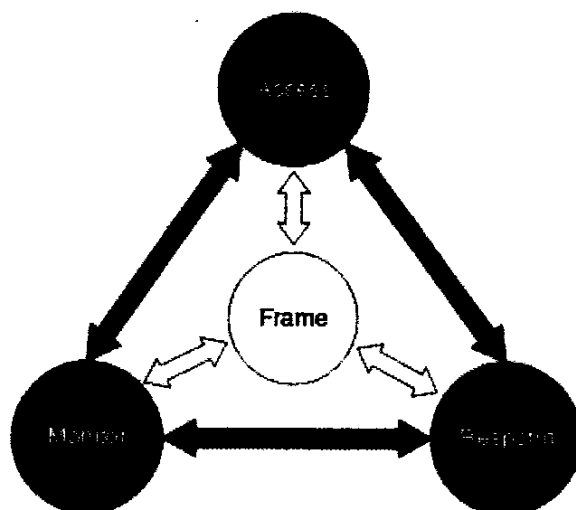


Figure 17. Risk Management. *Metrc's risk management process covers risk monitoring, assessment, and response.*

The risk framework describes the environment in which risk-based decisions are made. At Metrc, this is the impact that any issue may have on the System, regulatory enforcement, and/or ability to meet regulatory or legislative requirements. Because of the wide scope, the key stakeholders involved in risk management include the Metrc engineering team, program manager, client program manager, and executive leadership, depending on the severity.

Risk monitoring includes the proactive steps taken to ensure that the impact of external (e.g., new legislation) or internal (e.g., a System improvement) changes are controlled. It also includes reactive monitoring, such as in the case of a user-reported issue.

Risk assessment refers to the analysis and prioritization of those risks once identified. Depending on the initial assessment, risks may be escalated to leadership for further review. Metrc typically assesses:



- Scope (e.g., system performance, UX, security)
- Severity (e.g., showstopper)
- Number of users affected
- Other systems affected

Risk responses are dependent on the assessment and are documented and owned by the program manager, including any mitigation activities and updated reports to relevant teams.

CASE STUDY 2 – ON-TIME DELIVERY ACHIEVED WITH RISK MANAGEMENT & COLLABORATION

In a previous project, Metrc proactively identified that an external licensing system would not be ready for integration into the System prior to our target go-live date. We assessed that this was a high-impact and high-severity risk that would, unless addressed, cause a delay in implementation. We shared this among internal and external stakeholders and began developing a mitigation strategy in collaboration with our client agency, engineering team, program manager, and executive leadership.

After evaluating possible solutions for level of effort, system impact, reliability, and timeline, we proposed our best recommendation to the client agency: enable the upload of CSV files with licensee information until the licensing system was integrated into the Metrc System.

Following the client agency's approval and Metrc development, the agreed-upon solution enabled the System to be launched on time and with minimal adverse impact to our client agency.

Communication Resources

Metrc's communication and resource management approach includes a Communication Management Plan and Teamwork, our collaborative project management tool.

The Communication Management Plan establishes how communications with project team members, project stakeholders, senior staff, and the public (if appropriate) will be handled throughout the project lifecycle. It defines:

- Change process
- Change responsibility
- Communications execution
- Communication tracking
- Public relations

The online project management tool, Teamwork, provides the source of record for project resources and commitments, including schedules, RAIL (Recurring Action Item List) documents, project milestones, shared documents, release plans, testing documents, and training materials. And our communication management builds upon that material, providing updates,



risks, and obstacles that reference the shared resources housed in Teamwork and reviewing them on regular calls.

Issue Management and Escalation Process

Metrc follows a well-defined issue management and escalation process consisting of six steps:

1. **Identification:** Project staff members or end users typically identify issues during meetings, analysis, document reviews, workgroups, and other project activities. The Metrc Program Manager documents and escalates identified issues in meeting minutes and enters them into the correct reporting vehicle, such as the weekly RAIL, Backlog, SOW, or other reporting tool.
2. **Validation and Prioritization:** Metrc and State project staff review the issue and follow a documented process for review. In the next weekly meeting, Metrc and State staff discuss its priority, confirm the assignment, and establish a due date.
3. **Analysis:** The Metrc Program Manager assigns a team member to perform the required analysis to close the issue. The assignee provides periodic status updates. The analysis will determine the following for project scope management:
 - Impacts to project scope
 - Impacts to the schedule
 - Impacts to resources
 - Risks
 - Resolution/options
 - Escalation
 - Closure
4. **Escalation:** The Escalation Process ensures that critical issues are raised before they can impact the project schedule, key stakeholders, or end users and that the appropriate parties are informed and involved in the decision-making process.
5. **Tracking and Reporting:** Issues, progress, risks, and resolutions are tracked in the RAIL and other appropriate documentation, such as SOW, Backlog, Project Schedule, or Fit/Gap analysis.
6. **Resolution:** The Program Manager ensures that the resolution has been met, appropriate actions have been taken, and all key stakeholders are satisfied with – and sign off on – the outcome.



3.5d: Training Plan

The vendor must provide a training plan for both internal and external users. Training plan should include the following items and estimated completion: timeframe for each of the item:

Training Needs Analysis: topics should include but not limited to the following:

1. System configuration
2. User Administration
3. Security Features
4. Password Reset Instruction
5. Functionality related to the inventory and chain of custody management for the manufacturer, transportation, testing, distribution, recall tracking, sale, and reporting.
6. Reporting Features
7. For technical staff, the use of the platform API
 - Role Based Training Materials
 - Webinar Based Training
 - End User Manual and Material Updates:
 - Periodic Training Assessment Review

We develop a Training Plan for the State that includes internal and external users as part of the project management process. The Training Plan will include a proposed training schedule, which we will fine-tune collaboratively during the project kick-off meeting. Below is a sample approach for our training plan:

Task	Timeframe
System Configuration	ASAP after Kick Off
Train SD State Program Leads	ASAP after Kick Off
Initial Intro for Licensees – Roadshow	60 days prior to Go-Live
New Business Classes (including System Security, Password Resets, basic functionality & reporting)	15-30 days prior to Go-Live and beyond
State User – Intro to Metrc Training (including System Security, Password Resets, basic functionality & reporting)	15 - 30 days prior to Go-Live and beyond
Testing Facilities Intro Training	15 - 30 days prior to Go-Live and beyond
Advanced License-Specific Training	At Go-Live date and beyond
Testing Facilities Advanced Training	30 + days from Go-Live

System Training Program

Metrc's support and training teams' driving goal is to ensure State staff and licensees can use the System effectively and with ease. This starts with a highly qualified support and training staff, extends to a comprehensive training program, and continues with ongoing, unlimited support.

Metrc training team members are all full-time, U.S.-based Metrc employees. We do not outsource our training. Metrc's user training program is designed to ensure that State and



licensee users can work proficiently on the Metrc System. User training is unlimited and offered at no additional cost to users or the State.

State User Training

The State's training program will meet interdepartmental needs, such as field investigations, tax audits, and regulatory compliance, and accommodate potential users from other agencies such as Tax, Agriculture, Health, and Consumer Safety. This approach ensures that all stakeholders can effectively leverage the System if desired by the State.

State user trainings cover various topics including, but not limited to:

- **System Configuration** – item categories, state user roles, test category batches, action reasons, remediation and plant waste methods, and transfer and waste types
- **User Administration** – username and password, password security, changing a password, and guidance on how to lock users accounts during vacation or extended leave.
- **Security Features** – session timeouts during periods of inactivity, multi-factor authentication.
- **Password Reset Instruction** – procedures for password resets, security questions, changing email addresses.
- **Basic Inventory Functionality** – chain of custody, transfers, testing, recalls, sales, and reporting.
- **Reporting** – basic reports; including functional type canned reports (facility, plants, harvests, transfers, packages, adjustments, lab testing, and sales) as well as specific reports written in SQL query language.
- **Technical Training on API** – uniqueness of API keys per user and integrator, two-key system, process of creating an API key, and how to maintain chain of visibility.
- Should there be any other requirements beyond this we will be glad to incorporate this into our training and it should be able to become effective within the time the state wishes.

The training program includes online and in-person components, alongside presentation-style and hands-on classes. The following details the types of training Metrc offers for State users:

State Workshops: Before the System is deployed in South Dakota, we offer a series of high-level overview workshops for both local and remote State staff as well other stakeholders who will not be using the System (e.g., lawmakers, law enforcement, etc.) but may want to understand what the System does. These workshops focus on key System components and benefits and often provide context on cannabis regulations.

Workshops are typically hosted in-person but can be recorded and made available online.

Training Classes: These hands-on classes are designed to educate State staff who will be users of the System's agency-facing functionality. They provide step-by-step walkthroughs of essential functionality, often in a non-production environment where employees can work in a



“live” System environment, perform functions, and review how the System works using testing data. Classes are customized based on the State’s unique departments and the specific job functions of class attendees. For example, a field investigator would require a different understanding of the System’s available functions than would a tax auditor.

Testing Access: While formal training is the start of the knowledge-transfer process, we find that the more hands-on experience users get, the better they learn. Because of that, we provide State users with access to a State-specific testing environment. This enables them train and explore the System on their own (as well as perform user acceptance testing and performance evaluations). Providing an environment for new users to experiment with on their own greatly reinforces and supplements the more formalized training classes.

User Acceptance Testing (UAT): UAT is primarily intended to test System functionality and ensure that it meets business requirements, but it also presents an opportunity to teach users about new features. The UAT process allows for a systematic approach to understanding every core aspect of the System. By involving multiple departments and disciplines in UAT, we increase buy-in and reinforce understanding of the System.

In addition to the training methods described above, Metrc facilitates site visits to licensed facilities. These collaborative events can dramatically improve the State’s understanding of how the System is used by the industry and give context to the data that State users will be viewing. Metrc will work with the State to approve and schedule a series of regional site visits with your designated team.

To help the State confirm that trainings have been successful and users have achieved System competency, Metrc provides an online testing resource. The State can use existing tests or create new tests that can be assigned to all users.

Training Materials

While we customize courses and materials to meet each agency’s specific needs, the following table demonstrates the typical training materials we provide to agency and licensee users.

Material	Method	Duration
Agency Manual	Printable PDF	Provided at time of contract
Industry Manual	Printable PDF	Provided at time of contract
Industry Supplemental Guide	Printable PDF	Provided at time of contract
Handheld RFID Device Manuals	Printable PDF	Provided at time of contract
PowerPoint Training Presentation	Printable PDF	Provided at time of contract
Weekly Admin Training Webinar	Web Based	Registration on Metrc.com
Weekly Associate Training Webinar	Web Based	Registration on Metrc.com
Personalized/Company Webinars	Web Based	Upon request
Sandbox Environment	Web Based	Upon request



Support Email	Email/Printable	Support@metrc.com
Support Desk	Phone	Provided at time of contract
Support Ticket Reference	Email/Printable	Provided at time of contract
Admin System Updates	Email/Printable	Metrc Admin – Provided at time of contract

Licensee User Training

A successful track-and-trace program depends on licensees being able to use the System effectively to report product information. To support that need, Metrc provides a dedicated training staff and comprehensive training program for licensees.

Our experienced team has successfully implemented customized training programs for 16 jurisdictions and has educated thousands of users on Metrc System usage. In 2020 alone, we offered over 2,000 training sessions on the System for users across the United States. And our YouTube tutorials have been viewed over 80,000 times. We've also recently launched an interactive Learning Management System (LMS) to further supplement the online training experience for users.

To support the State, Metrc will deliver a training program that spans from introductory courses for new users to more advanced courses that are customized for State-specific license types. Trainings are delivered in a variety of ways, including in person, through live webinars, and via self-paced e-learning. In addition, we provide both digital and printed training materials. While we support licensee users by training them on using the Metrc System, we do not offer training related to other topics, such as business operations or broader regulatory compliance.

At the start of the training program, Metrc training team members collaborate with the State to understand the various groups who will need trainings (e.g., licensee owners/administrators, licensee staff, third-party integrators, etc.). They then develop and customize training content for each.

Licensee users advance through the following trainings to achieve proficiency in the System:

Industry Workshops: Before the System is deployed in South Dakota, we offer a series of workshops for licensees with the aim of providing an understanding of what Metrc is and what it does. To that end, workshops include a complete walkthrough of the System's functionality via discussions, demos, and hands-on exercises. They also include a question-and-answer period at the end. Workshops are typically designed for a general audience of all licensees but can also focus on specific license types. They are instructor led and leverage the testing environment of South Dakota's Metrc System instance.



Workshops are usually offered in a series of three to five sessions and are approximately three hours long. They can be offered twice a day as the System deployment date approaches.

We schedule workshops in various locations across South Dakota to maximize the number of attendees. If travel or in-person workshops are not advisable or permitted, we will host them online. Metrc will work with the State to identify, secure, and schedule the required facilities as part of the training and deployment plan.

New Business Metrc Training: Once the System is deployed, licensees must become certified to use the System. To become certified, licensees and employees who will be using the System must complete the New Business Metrc Training. This webinar-based training is instructor led. It provides a walkthrough of the System's functionality, covering all aspects of data required for accurate reporting of cannabis-supply-chain activities, and includes an interactive question-and-answer session. It can be offered any weekday (except on observed holidays) as the System deployment date approaches—sessions can be recorded and hosted online for later viewing.

Advanced Training: Once licensees are credentialed to use the System, they can take more advanced courses focused specifically on their individual license types (e.g., Cultivation, Manufacturing, Distribution, Transporter, Testing, Dispensary/Retailer, etc.). These advanced trainings are webinar based and instructor led and include a question-and-answer session at the end. Metrc will work with the State on an ongoing basis to identify any processes or topics that may need "extra attention" and develop advanced training courses to support and improve competency in those areas.

Function-Specific Trainings. Users can also get highly specific functionality trainings via YouTube videos. These are available to licensees anytime, on demand. The videos are short (five to eight minutes long), focus on specific System functions, and offer step-by-step instructions for completing a very focused process step. They allow users to easily find solutions to specific obstacles they may be facing without having to sit through a full-length course.

Testing: We provide competency testing to evaluate user mastery of the System. The tests are available online and are accessed via the user portal (see Figure 18). They cover specific System actions and are tailored to the State's license types. All test results are reported back to the State and identify any gaps in knowledge and usage that need to be addressed.



When Adding an Employee in Metrc, make sure their home page is:

☐ always Admin

☐ any area will do

☒ an area you have given the employee permission for



Figure 18. Metrc Training Question. *Metrc's online quizzes ensure that training attendees absorbed the requisite knowledge to be proficient in the System.*

Learning Management System: Licensees will have a central location for all of their Metrc training needs via Metrc Learn, our newly released interactive Learning Management System (LMS). Metrc Learn will supplement our current training program by giving licensee users all the on-demand training they want and need (Figure 19).

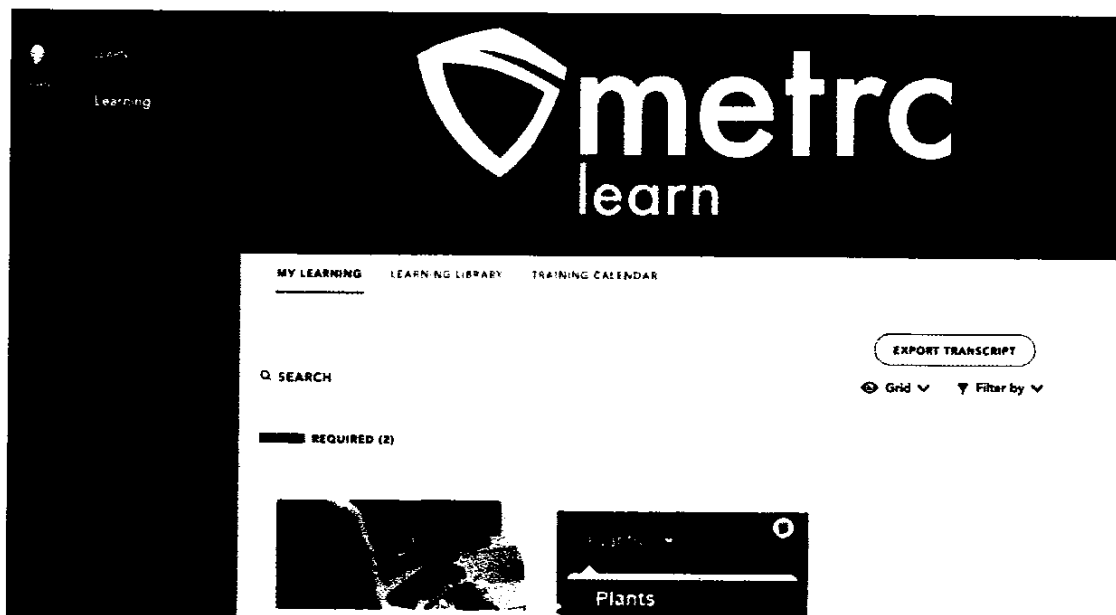


Figure 19. Centralized Training Platform. *Learners will have all the tools needed for comprehensive, role-specific training at their fingertips.*



Metrc Learn is organized into role-specific programs that are made up of various courses; each course is focused on one function in Metrc and includes a demo and a hands-on component (Figure 20). Users can either self-select or be assigned programs and can take each course at their own pace. This approach gives users the flexibility to learn about other areas of the System that may interest them, as well as the ability to see what courses are mandatory for their role. Once users complete all courses in a program, they take a comprehensive quiz that they must pass (scoring 70% or higher) before the program is considered complete.

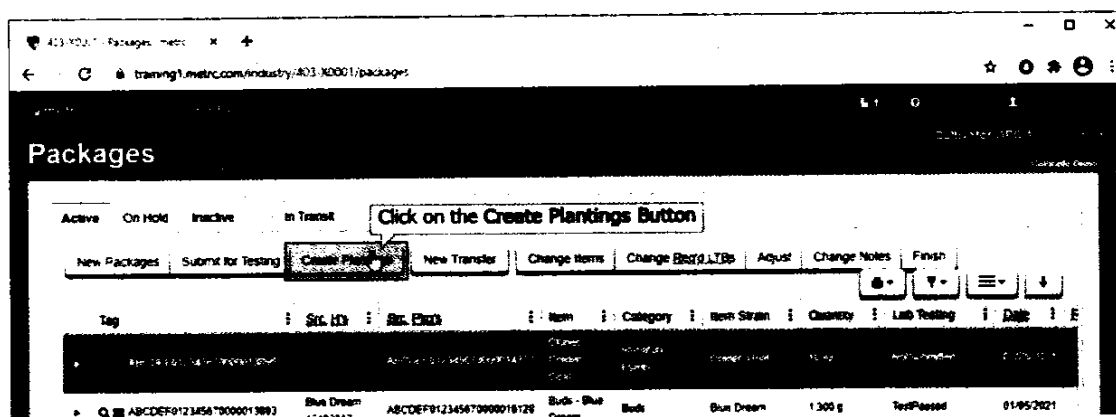


Figure 20. Hands-On Trainings. Trainings include audio and visual instructions and give learners the opportunity to perform tasks on their own, as many times as desired.

Metrc Learn tracks and displays all completed coursework. It even issues badges and certificates upon completion of a program that users can post on their social media. And, if they want, they can print out a transcript of all their training to provide for future employers. Users can also explore the Learning Library within Metrc Learn—and its many dozens of YouTube videos and resources—or find webinars they'd like to attend via the Training Calendar.

Metrc Learn also provides advanced reporting and analytics. In easy-to-understand graphs and charts, it shows course and program completion rates, learner progress, group size, courses offered, most popular courses, and more (Figure 21). Every graph and chart provide an overview as well as the ability to drill down to granular details and print findings. The State will have access to these reports. You will be able to see all training courses for every license type within your jurisdiction and can receive scheduled, automated reports detailing training progress throughout South Dakota.

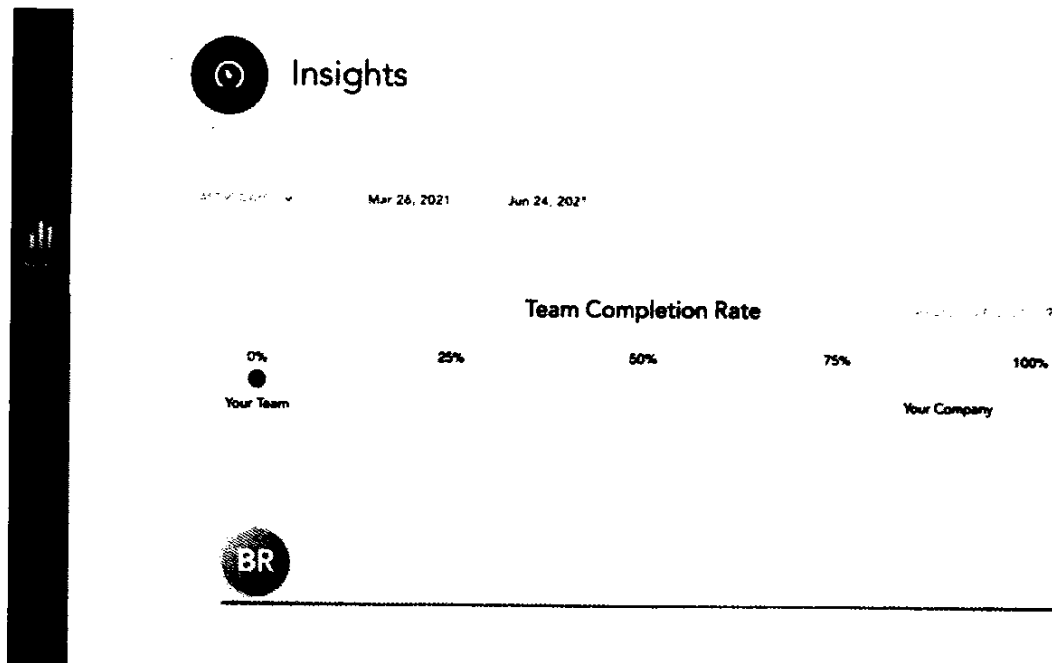


Figure 21. Training Analytics. *The State and licensee will have full insight into training progress and much more.*

IV.c. Options or Alternatives Proposed

Metrc is proposing the following alternatives:

Lab Documents – The Metrc System has the ability to allow testing facilities to upload their certificate of analysis documents (COAs) to associate it with the tested package and any associated packages with the test sample. These documents would be stored in PDF and would be available to any licensee with the package to allow full transparency of the test results throughout the supply chain.

Item Photos – The Metrc System has the ability to allow industry users to associate photos with items they create. There are three photo slots available: product photo, label photo, and packaging photo. This feature allows State users to view the items that are being created by the licensees and can be used to populate the Metrc System Catalogue if enabled.

Item Approval Process – The Metrc System has functionality that allows for State users to review and approve items entered by licensees before they are available to be used in Metrc. This process allows State users to ensure that items are being created in accordance with regulations. If items are not acceptable, State users can make notes on the note as to why it is being rejected before sending it back to the licensee to address the issue.



Handheld RFID Readers – To support the State’s field audits and inspections of marijuana facilities, Metrc offers the **optional lease of two handheld RFID readers at no cost (\$0)** for the term of the contract. If the State wishes to lease additional RFID readers from Metrc at any point in the contract term, Metrc will provide the State with the option to do so. The lease program minimizes costs and enables Metrc to upgrade readers as needed, always keeping pace with new software or hardware developments in the RFID industry.

If the State chooses to exercise those options, Metrc will include the following with each handheld device at no additional cost:

- Pre-installed, fully configured and tested software (Investigator App); units are ready to use right out of the box.
- Seamless integration into Metrc’s traceability (track-and-trace) system.
- Software and device training and support, including documentation for all client users.
- Replacement of damaged units or parts, as covered by warranty.
- Repair of damaged units or its parts, as covered by warranty.
- Replacement of outdated devices and software.



V. Cost Proposal

APPENDIX B – Cost Sheet

1. Basic Cost: the cost for this section should cover the implementation and ongoing maintenance and support for all the requirements outlined in Section 3.1 through 3.5 of this RFP.

	State Cost	Amount
Implementation Cost		
	Product Cost	\$0
	License Cost (Specify below)	\$0
	Other Implementation Costs (Specify below)	\$55,000
SaaS Cost		
	Year 1	\$20,000
	Year 2	\$75,000
	Year 3	\$75,000
	Year 4	\$75,000
	Year 5	\$75,000
	TOTAL:	\$320,000

	Cannabis Establishment Cost	Amount
Implementation Cost		
	Product Cost	\$0
	License Cost (Specify below)	\$0
	Scanner for Identification Tag or Label	\$0
	Cost per Tag/Label	\$0.45 per plant tag \$0.25 per wholesale package tag
	Other implementation Costs (Specify below)	\$0
Maintenance and Support Cost		
	Year 1	\$480/year (\$40/mo.) per credentialed license
	Year 2	\$480/year (\$40/mo.) per credentialed license
	Year 3	\$480/year (\$40/mo.) per credentialed license
	Year 4	\$480/year (\$40/mo.) per credentialed license



	Year 5	\$480/year (\$40/mo.) per credentialed license
	TOTAL	\$2,400 per credentialed license

2. Cost Proposed by Deliverables: This section is to understand the cost by deliverables. The deliverable expectation and details are included in Section 9.2 of the RFP.

Deliverable	Cost
1. Kickoff	\$1,500
2. Project Plan	\$3,500
3. Gap Analysis	\$5,000
4. System Configuration	\$10,000
5. Acceptance Testing	\$10,000
6. Training	\$5,000
7. Implementation	\$20,000

3. Cost Structure Explanation: Please provide an explanation of the cost structure and its cost per unit or tier.

	State Cost	Cannabis Establishment Cost
License Cost: Explanation and cost per License or Per Tier. If the cost per license changes based on market size (i.e. sales) please include the cost structure based on scale.	The pricing presented above is the all-inclusive ^{1,2} cost to the State for the System, regardless of license quantities and is intended to support both the medical and adult-use programs.	Licensed businesses will be charged a monthly reporting fee to access and use the system. ³ The reporting fee is \$40 per license per month (PLPM) and is not assessed until the license's admin has been credentialed into (i.e., has been granted access to) the system. Metrc proposes that the reporting fee be eligible for annual CPI increases which will be preceded by a 90-day advanced notice from Metrc.

¹ Our all-inclusive cost to the State includes hosting; system configuration, integration, and implementation; agency user access; reporting and data downloads; unlimited training and support; and two RFID handheld units for facility inspections. (Additional handhelds are available for lease at for \$100 per unit per month)

² This pricing also includes an optional lease for two handheld RFID readers for the term of the contract. If the State wishes to lease additional RFID readers from Metrc, Metrc will provide the State with the option to do so. The lease program is designed to minimize the cost while providing Metrc the ability to upgrade the readers as needed to keep pace with new software or hardware developments in the RFID industry

³ The fee includes user access, reporting, data downloads, open API integration, and training and support.



Tag/Label Cost: Cost per tag or label. If the cost per license change due to scale if the cost per license changes based on market size (i.e. number of plants) please include the cost structure based on scale.	There is no cost to the State for Tags/Labels. If the State desires to purchase tags on behalf of a/the Cannabis Establishments, the pricing would remain the same at \$0.45 per plant tags and \$0.25 per wholesale package tag plus all applicable taxes and shipping & handling. Metrc does not recommend this approach.	Licensed businesses must procure from Metrc the RFID tags used to track their products. The RFID tags cost \$0.45 per plant tag and \$0.25 per wholesale package tag. ⁴ Sales tax and shipping & handling charges are also the responsibility of the licensed business and will be assessed and charged by Metrc at the point of sale. Metrc proposes that the tag fees will be eligible for annual CPI increases which will be preceded by a 90-day advanced notice from Metrc.
Other Implementation Cost: Explanation and breakdown of costs associated with implementation	Implementation costs, as outlined in Appendix B Section 2, above, will be invoiced at the completion of each deliverable as agreed to by both Metrc and the State. Additional details on what each deliverable consists of can be found in IV.a.1 Approach and Methodology to Meet Project Requirements.	There are no implementation costs to licensees. The reporting fee is not charged until both the cannabis businesses are licensed by the State and the licensee is credentialed in the system. Licensees do not have to pay for any upfront costs and will receive all training, including the required training for credentialing, at no additional cost.

4. Optional Cost: the cost for this section should cover the implementation and ongoing maintenance and support for requirements that are labeled as optional. Any additional features that are unique to your proposal and the cost associated with them should be included in this section.

Optional Services Description	Dollar Amount
a. Lab Documents	\$6,000.00 / year for up to 100 GB of lab documentation storage (implementation and training is included)
b. Item Photos & Approvals	\$24,000 / year for up to 100 GB of photo storage (implementation and training is included)
c. Metrc Catalogue	\$24,000 / year for up to 100 GB of photo storage (implementation and training is included)
d. RFID Handheld Readers (max 2)	\$0 each

⁴ In any track-and-trace solution, unique-identifier tags are a necessary, critical component to track product. Metrc's proprietary tags are a critical component of our complete (and, in our opinion, best-value) solution. Metrc provides for in-house production and provisioning of these tags, meaning we centrally produce them at scale. This affords several benefits to both industry and the state, including ease, quality, consistency, and cost.



e. RFID Handheld Readers for Purchase	\$1,588 each + \$156 / year for Spector App and Reader Maintenance
f. RFID Handheld Readers for Lease	\$1,200 / year (includes Spector App and Reader Maintenance)

Information on each of these optional services is included in **Section IV.c. Options or Alternatives Proposed.**



Metrc Cost Proposal Narrative

Introduction

Metrc is fully willing and able to perform the work described in this RFP for the price being offered in Appendix B – Cost Sheet. To provide additional information on the costs itemized there, we are providing this pricing narrative to help explain our pricing model.

At Metrc, we pride ourselves on the transparency of our pricing and our affordability for both government and industry users alike. We seek to minimize the cost of our solution to both client agencies and businesses, and we ensure that these costs are straightforward and equitable. There are no hidden or large one-time costs, and our industry fees are designed to be proportionate to the size of the business.

State Costs

Metrc is determined to keep our system as affordable as possible for the State of South Dakota and is proposing a total annual cost of \$75,000.⁵ This amounts to a \$375,000 total cost to the State for all five years of the contract. To offset the first year's cost of deliverables, Metrc will discount the first year of hosting costs by \$55,000. This pricing includes the software licensing, software maintenance, hosting, help desk support, training, and reporting for State users required in this solicitation.

Metrc is mindful of the dynamic nature of implementing and enforcing cannabis policy. We understand that cannabis regulators may have conservative budgets, and public policy related to cannabis is likely to evolve significantly for the foreseeable future. Our approach to track-and-trace is designed to be both highly affordable and flexible to meet ever-changing requirements.

The all-inclusive, annual cost to the State helps pay for our annual hosting fees, while Metrc absorbs the cost of other services, such as system configuration and development, ongoing program management, and help-desk support and training for State users.

Additionally, our business model and pricing structure enable us to include the development, testing, and implementation of reasonable system enhancements at no additional cost. This includes changes requested by both our client agencies and industry users. Existing clients have told us that this is a significant benefit, given how frequently and quickly rules, regulations, and statutes can evolve—and how expensive change fees can be with other vendors.⁶ Metrc places our customers' needs at the forefront of our solution, and we ensure that changes can be easily incorporated into the system.

⁵ Metrc will begin charging the State this annual fee upon delivery of our test environment for state user access. Metrc proposes charging the State quarterly, with the first charge prorated based on the test environment delivery date.

⁶ For example, the State might decide over time to change or expand license types—or allow for home delivery. Based on our research, some vendors have charged other jurisdictions as much as \$50,000 for such changes. Metrc, however, considers such changes as reasonable system enhancements that are included under our contract at no additional cost.



As referenced above, Metrc includes the cost of all reasonable system enhancements in our annual fee and avoids change orders whenever possible. However, in rare circumstances, some clients have asked for system changes that were mutually determined to be out of scope and required a significant investment of labor and resources. In those instances, Metrc will bill for labor at the blended hourly rate of \$185 per hour. Any such charge will be reviewed and approved by the State prior to the start of work.

Lastly, additional information on Metrc's Optional Services is included in **Section IV.c. Options or Alternatives Proposed**.

Licensee Costs

Metrc charges set fees to licensees for system access and for our proprietary plant and package tracking tags. These fees are charged directly to licensees, are paid through the Metrc System, and enable licensees to access the system with unlimited users, while taking advantage of unlimited support and training.

Metrc's total costs to licensees are relative to the size of the business; this ensures that costs are equitable and helps small businesses that are just starting out. And, similar to our cost to the State, there are no hidden fees, expensive annual maintenance fees, or one-time setup charges. Fees are not charged until cannabis businesses are credentialed into—and are able to use—the system. There are no additional software or hardware components required to provide the full functionality included in our bid, outside of a computer with internet connectivity.

Licensee Reporting Fees

Cost: \$40 per month per license plus applicable state and local taxes.

Includes:

- Access to the system for associated licensee users
- Licensee user training (online and in person)
- Licensee user support (via phone and email)
- API access for integration of licensee enterprise software (e.g., ERP and POS software)

Licensee RFID Tracking Tag Fees

Cost: \$0.45 per plant tag and \$0.25 per wholesale (or lot) package tag plus applicable state and local taxes and shipping and handling charges.

Includes:

- Fast, expedited tag creation: historically, over 98% of Metrc tag orders have been ready to ship within 24 hours of order receipt.
- Hassle-free and ready-to-use tracking tags (no other equipment, materials or labor required for licensees).
- High-quality and consistent tags that are durability tested for harsh environments and



resistant to light, water, and chemicals.

- Embedded, encoded, and integration-ready RFID chips for licensee use, e.g., with RFID-readable scales and inventory monitoring hardware.

Conclusion

Metrc's leading track-and-trace system's cost structure is a tried and tested model that has worked successfully over the past 10 years, enabling and providing both industry and government agencies to use the leading track-and-trace system at with an affordable and consistent cost. Our approach:

- Incentivizes us to deliver a fully functional system that meets all our client requirements on time, since we have invested the initial capital to deploy the system and will not begin recouping it until the system is used by industry.
- Does not require government to budget large sums of money for a system during the early phase of implementation when tax revenues are uncertain.
- Ensures that the cost of the system remains proportionate to the size of the business, allowing smaller licensees to use a world-class inventory system at a fraction of what it would cost to purchase a similar system for their own use.

Metrc makes every resource available at the lowest possible cost to ensure a safe and effective medical and, if applicable later, adult-use cannabis market. Through this, Metrc's intent is to support the State's goal to create and operate a new regulatory program to ensure the safety of patients, students, and the public in this new industry.



VI. Metrc Hosted Security and Vendor Questions (Appendix D)

Metrc has completed the Security and Vendor Questions, attached as Appendix D, which is attached as a separate document to this proposal, as preferred by the State.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.



VII. List of Subcontractors

Metrc does not intend to use any subcontractors for this project.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.



VIII. Statement of Understanding of the Project

Overview

Metrc understands that The South Dakota Department of Health and South Dakota Department of Revenue are jointly issuing a request for proposal (ID #2439) to acquire a cannabis tracking system to be used to support the implementation of the South Dakota medical (and potentially adult-use) cannabis program. The State is seeking a vendor to provide a seed-to-sale tracking system that accommodates the program needs for medical Cannabis as well as the needs of an adult-use program. The adult-use track-and-trace component is dependent on the South Dakota Supreme Court's determination of the validity of Constitutional Amendment A. Although there are no statutory or constitutional deadlines related to the implementation of a seed-to-sale tracking system, the State requires an expeditious implementation regardless of the Supreme Court's decision and require an expedited six-month seed-to-sale tracking system implementation.

Through the seed-to-sale tracking system, the State will be able to track Cannabis plants and products from the cultivation of the individual cannabis plants to the eventual dispensary sale to an authorized medical cannabis consumer. It will be also able to securely identify the specific cannabis plants used for a manufacturing process that creates cannabis products. This, in turn, will enable the State to perform targeted product recalls that are later determined as not safe for consumption or use. Finally, the System will support the State in preventing the illegal diversion of cannabis or cannabis products into the illicit market and provide transparency and accountability within the industry. Ultimately, it will help the State ensure the safety, health, and welfare of South Dakotans.

Included Services for the Project

Metrc understands that the State is seeking qualified vendors to provide an affordable, complete, secure, and turnkey seed-to-sale system. "Qualified vendors" refers to the vendor's requisite experience and references to demonstrate prior successful delivery—and ability to continue doing so in the future. "Provide" means the vendor's ability to successfully plan, project manage, kick off, configure, implement, train, support, and manage the system for the duration of the contract. "Affordable" refers to the vendor's ability to provide its solution at a low, set, and transparent cost, both to the State and licensees. "Complete" refers to the vendor's ability to fulfill the 69 requirements detailed in section IV.b—and continue to meet requirements in the future as cannabis policy, rule, and law evolves over time. "Secure" refers to the ability of the vendor to provide the required cyber and physical security precautions to ensure that State and licensee data is not compromised, that system uptime is maintained, and that physical tracking tags are resistant to counterfeiting. "Turnkey" refers to the ability of the vendor to provide a proven and highly flexible system that can be quickly adapted to the State's unique rules and laws—and meet the State's six-month implementation timeline. And "seed-to-sale system" refers to a robust solution that provides the ability for licensee users to accurately report marijuana material and demonstrate compliance—and for State users



to monitor and govern that material as it moves through the supply chain—through physical tracking tags and, an easy-to-use online portal, and open API for seamless data exchange between systems.

Commitment to the Project

Metrc is committed to providing all deliverables and requirements associated with this RFP. Metrc is the most trusted and experienced provider of cannabis traceability ("track-and-trace" or "seed-to-sale") solutions in the United States, with government contracts in 15 U.S. states and the District of Columbia, where we diligently work to make sure our clients' cannabis regulatory programs are 100 percent successful. We provide best-in-class technology and support for both medical and adult-use marijuana markets that is proven to play a role in the shared goal of transparency, safety, and accountability. Furthermore, we are the only seed-to-sale vendor to successfully replace an incumbent vendor, having done so in both Maine and Nevada.

Our software, technology, and support teams track cannabis products from seed to sale, ensuring a closed, legal ecosystem. Our solution provides a safe marketplace with a transparent and secure supply chain. In the jurisdictions we serve, we have approximately 1,300 regulatory users and 220,000 licensee users across 30,000 licensed businesses. Our regulatory clients have tracked almost \$24 billion in sales and over 1 billion supply chain events, such as harvests, transports, test results, and final sale.

The State should rest assured that, should it select Metrc as its vendor, it will receive the most robust seed-to-sale platform available on the marketplace that will exceed its expectations and meet each of its project goals.



IX. Additional Forms/Appendices

APPENDIX A – Use Cases for Vendor Presentation

Metrc acknowledges that the use cases outlined in Appendix A of the RFP must be demonstrated by vendors invited to an oral presentation with the State. We are prepared to show the usability of our software regarding ease of use, product functionality, flexibility, and adherence to the use cases identified below:

- Role-Based Security
- Cultivator Tracking
- Manufacturer Tracking
- Product Transfer
- Product Testing
- Product Testing - Failed Products Communication
- Processing without Product Testing
- Dispensary Tracking
- Dispensary Tracking – Exceeds the allowable limit
- Patient Product Return
- Department Review of Inventory

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.



APPENDIX B – Cost Sheet

Metrc has included Appendix B in Section V., Cost Proposal.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.



APPENDIX C – Exceptions/Alternative Language for State Standard Contract and Bureau of Information and Telecommunications Required Contract Terms

Metrc does not take exception to RFP Section 2., Standard Contract Terms and Conditions, or to Appendix C, Bureau of Information and Telecommunications Required Contract Terms; however, Metrc is requesting that at time of contract award any references that do not apply to the final, negotiated solution will be removed (i.e., language specifically related to hosting on the State's infrastructure).

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.



APPENDIX E – Scanning Permission Form

APPENDIX E - Scanning Permission Form

The offeror acknowledges that the State will be able to do a security scan of the offeror's product or service. This will be a vulnerability scan that will not include a penetration test. The State will use industry standard tools. The State prefers to scan a non-production environment with non-production data. These scans will be done at mutually agreeable times. At the option of the State, a scan that demonstrates that the offeror's product or service meets the State's security requirements can be done either before an agreement between the State and the offeror is signed or after. The offeror should fill in the information below and sign this form authorizing the State to do a security scan. The offeror's employee signing this form must have the authority to commit the offeror to allowing the State to do a security scan. If no security contact is given the State will assume that the State can scan at any time. Any RFP response that does not include this signed form will be considered incomplete and may be excluded from further consideration.

Offeror's name: Metrc LLC

Offeror's security contact's name: Jesse Naranjo, Chief Product Officer

Security contact's phone number: (305) 586-2636

Security contact's email address: Jesse.Naranjo@Metrc.com

Web address URL or product name www.Metrc.com The State will contact the security contact listed above to arrange for a test log in for the scanning.

Offeror's employee acknowledging the right to scan (Print): Jesse Naranjo

Title: Chief Product Officer

Date: August 23, 2021

Signature: 



APPENDIX F – Security Acknowledgement Form

Metrc is including the signed Security Acknowledgement Form on the following page; however, we are noting two exceptions that we would request to discuss further with the State.

1. The requirement to prohibit password reuse for 24 generation (pg. 48) is against most recent explicit guidance from NIST 800-63B in 2020.
2. The requirement for reCAPTCHA (pg. 49) is not used by Metrc because the Metrc System will lock out users that fail to login three times for 15 minutes.



APPENDIX F – Security Acknowledgement Form

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy")**. Users are responsible for compliance to all information security policies and procedures. By signature below, the employee or contractor hereby acknowledges and agrees to the following:

1. Employee is a State of South Dakota employee or contractor that uses non-public State of South Dakota technology infrastructure or information;
2. Employee or contractor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Employee or contractor agrees to follow state and federal regulations in regard to confidentiality and handling of data;
4. Employee or contractor has read and agrees to abide by the Policy;
5. Employee or contractor consents to discuss with a supervisor / State contact regarding Policy violations;
6. Employee or contractor shall abide by the policies described as a condition of continued employment / service;
7. Employee or contractor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Employee or contractor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and contractors for the State to regularly review the appropriate Policy and annual amendments.

Information Technology Security Policy – BIT: <http://intranet.bit.sd.gov/policies/>

Information Technology Security Policy – CLIENT: <http://intranet.bit.sd.gov/policies/>

Information Technology Security Policy – CONTRACTOR: <http://bit.sd.gov/vendor/default.aspx>

Acknowledgement: State of South Dakota Information Technology Security Policy

Contractor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

8/23/2021

Employee or Contractor signature Date

BIT Manager or Contact

Date

Jesse Naranjo, Chief Product Officer, Metrc LLC

Employee or Contractor name and Company name in block capital letters



APPENDIX G – Business Associate Agreement

Since Metrc is not capturing or storing PII, the Business Associate Agreement, including HIPAA, should not apply. Metrc is requesting to further discuss this with the State, if needed.

THE REMAINDER OF THIS PAGE IS INTENTIONALLY BLANK.

Exhibit B

Bureau of Information and Telecommunications

Required Contract Terms

1. CONFIDENTIALITY OF INFORMATION

For purposes of this paragraph, "State Proprietary Information" shall include all information disclosed to the Vendor by the State. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or third party Vendors except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this agreement. The Vendor, and Vendor's Subcontractors, Agents, Assigns, and/or Affiliated Entities are held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State, destroyed, deidentified for internal reporting and Metrc use only or to the extent that it cannot be recalled or reproduced. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities agree to return all information received from the State to State's custody upon the end of the term of this agreement, unless otherwise agreed in a writing signed by both parties and as except specified in the Vendor contract, specifically wherein the State grants vendor the unrestricted right to retain and use such information and materials in the normal course of vendor's business for any lawful purpose. State Proprietary Information shall not include information that:

- (i) was in the public domain at the time it was disclosed to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities;
- (ii) was known to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction at the time of disclosure from the State;
- (iii) that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;

- (iv) was independently developed by the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without the benefit or influence of the State's information;
- (v) becomes known to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction from a source not connected to the State of South Dakota.

The State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Vendor understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. Vendor acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

2. CYBER LIABILITY INSURANCE

The Vendor shall maintain cyber liability insurance with liability limits in the amount of \$10 million dollars to protect any and all State data the Vendor receives as part of the project covered by this agreement including State data that may reside on devices, including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. Such insurance coverage is conditioned on the following: Vendor shall have a cyber liability insurance policy with a coverage limit of \$5 million, and two follow form policies of \$2.5 million each. The coverage above \$5 million is conditional on the State using Vendor's Multi-factor Authentication functionality to mitigate risk.

If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this agreement, then the Vendor shall include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under

this Agreement, the Vendor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement and which provide that such insurance may not be canceled, except on 30 days prior written notice to the State. The Vendor shall furnish copies of insurance policies if requested by the State. The insurance will stay in effect for 2 years after the work covered by this agreement is completed.

3. CHANGE MANAGEMENT PROCESS

From time to time it may be necessary or desirable for either the State or the Vendor to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Vendor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Vendor on a schedule no less favorable than that provided by the Vendor to any other customer receiving comparable levels of services.

4. WORK PRODUCTS

The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished by the Vendor and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Vendor to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Vendor shall, without additional compensation, correct or revise any errors or omissions in its work products.

Vendor hereby acknowledges and agrees that all State Proprietary Information, any information discovered by the State, Personally Identifiable Information (PII), data protected under Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information defined under state statute as confidential, and all information contained therein provided to the State by the Vendor in connection with its performance under this Agreement shall belong to and is the property of the State and will not be used in any way by the Vendor without the written consent of the State.

5. PRODUCT CONFORMITY

The State has one-hundred eighty (180) days following final acceptance of the product(s) delivered by the Vendor pursuant to this Agreement to verify that the product(s) conform to the requirements of this Agreement and perform according to the Vendor's system design

specifications, as detailed in the Fit/Gap Analysis provided by the Vendor and approved by the State during Phase 1 of implementation. Upon the State's recognition of an error, deficiency, or defect, the Vendor shall be notified by the State. The notification shall cite any specific deficiency (deficiency being defined as the Vendor having performed incorrectly with the information previously provided by the State, not the Vendor having to modify a previous action due to additional and/or corrected information from the State). The Vendor, at no additional charge to the State, shall provide a correction or provide a mutually acceptable plan for correction within thirty-days following the receipt of the State's notice to the Vendor. If the Vendor's correction is inadequate to correct the deficiency, or defect, or if error recurs, the State may, at its option, act to correct the problem. The Vendor shall be required to reimburse the State for any such costs incurred or the State will consider this to be a breach of the agreement. Payment by the Vendor pursuant to this provision does not waive any other rights and remedies available to the State.

6. CURING OF THE BREACH OF AGREEMENT

In the event of a breach of these representations and warranties the State may, at the State's discretion, provide the Vendor with the opportunity to rectify the breach. The Vendor shall immediately, after notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Vendor's request, a written notice to reaffirm the telephonic notice. If such problem remains unresolved after three days, at State's discretion, Vendor will send, at Vendor's sole expense, at least one qualified and knowledgeable representative to the State's site where the system is located. This representative will continue to address and work to remedy the deficiency, failure, malfunction, defect, or problem at the site. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

7. DOMAIN NAME OWNERSHIP

Any website(s) that the Vendor creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Vendor is providing a service that utilizes a website with the domain name owned by the Vendor, the Vendor must give thirty (30) days' notice before abandoning the site. If the Vendor intends to sell the site to another party the Vendor must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Vendor or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

8. SOFTWARE FUNCTIONALITY AND REPLACEMENT

The software licensed by the Vendor to the State provides the following functionality: The Vendor's software will enable the tracking of cannabis plants from seed to eventual purchase by consumers, including tracking and product management at all points along the supply chain.

The Vendor agrees that:

- A. If in the opinion of the State the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or renamed product, the State shall be entitled to license such software product at no additional license or maintenance fee.
- B. If in the opinion of the State the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

9. SERVICE BUREAU

Consistent with use limitations specified in the agreement the State may use the Product to provide services to the various branches and constitutional offices of the State of South Dakota as well as county and city governments and school districts. The State will not be considered a service bureau while providing these services and no additional fees may be charged unless agreed to in writing by the State.

10. LICENSE GRANT

- A. The Vendor grants to the State an annual, worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this agreement.
- B. The license usage model is based on an unknown number of state users and an unknown number of private business users.
- C. The license grant may be extended to any contractors, subcontractors, outsourcing Vendors and others who have a need to use the software for the benefit of the State.

11. SOURCE CODE ESCROW

- A. Deposit in Escrow: "Source Code" means all source code of the Software, together with all commentary and other materials supporting, incorporated into or necessary for the use of such source code, including all supporting configuration, documentation, and other resource files and identification by Vendor and version number of any software (but not a license to such third-party software) used in connection with the source code and of any compiler, assembler, or utility used in generating object code.
- a. Within ninety (90) days of the effective date, Vendor shall deposit the Source Code for the software with a nationally recognized software escrow company (subject to the approval of the State, not to be unreasonably withheld) (the "Escrow Agreement"). Within thirty (30) days after delivery to Customer of any major update, Vendor shall deposit the Source Code for such update with the Escrow Agent pursuant to the Escrow Agreement. For all other updates, Vendor shall deposit the Source Code for such updates on a semiannual basis with the Escrow Agent pursuant to the Escrow Agreement.
 - b. The parties agree that the Escrow Agreement is an "agreement supplementary to" the Agreement as provided in Section 365(d) of Title 11, United States Code (the "Bankruptcy Code"). Immediately upon termination of this Agreement, the Source Code shall be released back to Vendor.
- B. Conditions for release: The State will have the right to obtain the Source Code in accordance with and subject to the terms and conditions of this Section and the Escrow Agreement provided that all of the following three conditions are met (collectively a "Release Event"):
- a. Vendor winds down its business or liquidates its business under a Chapter 7 Bankruptcy proceeding; or Vendor discontinues maintenance and support to the Software,
 - b. No entity has succeeded to Vendor's obligations to provide maintenance and support on the Software in accordance with the Agreement in effect between the parties, and
 - c. The State is not in breach of its obligations under this Agreement.
- C. Source Code: In no event shall the State have the right to use the Source Code "barring a release event" for any purpose, and the State is specifically prohibited from using the Source Code to reverse engineer, develop derivative works or to sublicense the right to use the Source Code to any other person or entity for any purpose. Customer will also be obligated to treat the Source Code as Confidential Information of Vendor under the Agreement.
- The cost for establishing and maintaining the Escrow Account will be that of the State.

12. FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT

The Parties agree that the State shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

13. DATA RECOVERY

The Consultant must be able to recover the State's data in the same state it was sent to the Consultant for 13 months. If the Consultant system or the third-party system that is hosting data for the Consultant is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the State data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the State and the Consultant.

14. REJECTION OR EJECTION OF VENDOR AND VENDORS SUBCONTRACTORS, AGENTS, ASSIGNS, AND/OR AFFILIATED ENTITIES EMPLOYEES

The State, at its option, may require the vetting of the Vendor, and any of the Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities. The Vendor is required to assist in this process as needed.

The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor shall immediately remove the individual from the project.

15. PROVISION OF DATA

Upon notice of termination by either party, the State will be provided by the Vendor all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Vendor with all current State Data in a non-proprietary form. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

16. THREAT NOTIFICATION

Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Vendor.

17. SECURITY INCIDENT NOTIFICATION

For protected non-health information only, the Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policies found at: <https://bit.sd.gov/vendor/default.aspx>. The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

- A. The Vendor shall notify the State Contact within twenty-four (24) hours of the Vendor becoming aware that a Security Incident has occurred. If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twelve (12) hours after law-enforcement provides permission for the release of information on the Security Incident.
- B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all

of the available information along with the reason for the incomplete notification. A delay in excess of twenty-four (24) hours is acceptable only if it is necessitated by other legal requirements.

- C. At the State's discretion, the Vendor must provide to the State all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the Security Incident; (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered; (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred; and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none, use AES256 encryption. Vendor shall use the term "data incident report" in the subject line of the email. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.
- D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person Vendor must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Vendor shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Vendor is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Vendor reasonably determines that the breach will not likely result in harm to the affected person. The Vendor shall document the determination under this section in writing and maintain the documentation for not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and Vendor shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

18. HANDLING OF SECURITY INCIDENT

For Security Incidents of protected non-health information under the Vendor's control and at the State's discretion the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

- (i) fully investigate the incident,
- (ii) cooperate fully with the State's investigation of, analysis of, and response to the incident,
- (iii) make a best effort to implement necessary remedial measures as soon as it is possible and,
- (iv) document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

If, at the State's discretion the Security Incident was due to the actions or inactions of the Vendor and at the Vendor's expense the Vendor will use a credit monitoring service, call center, forensics company, advisors, or public relations firm whose services are acceptable to the State. At the State's discretion the Vendor shall offer 3 years of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Vendor, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense.

If the Vendor is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twelve (12) hours of the investigation report being completed. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Vendor shall also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

19. ADVERSE EVENT

The Vendor shall notify the State Contact within two (2) days if the Vendor becomes aware that an Adverse Event has occurred. An Adverse Event is the unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. If the Adverse Event was the result of the Vendor's actions or inactions. The State can require a risk assessment of the Vendor the State mandating the methodology to be used as well as the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

The Vendor also acknowledges that if not kept secure, the State's data could be, in aggregate, used for illegal purposes.

Except as mandated by other legal requirements the Vendor shall provide notice of the disclosure only to the State. Notification to the State of an Adverse Event involving the disclosure of State Data shall consist of a description of the data disclosed, the time the disclosure occurred, and a general description of the circumstances of the disclosure.

If all this information is not available for the notification within the specified time, the Vendor shall provide the State with all the available information along with the reason for the incomplete notification.

The parties agree with respect to any Adverse Event that the Vendor shall at its sole expense:

- A. Promptly and fully investigate the cause of the Adverse Event;
- B. Cooperate fully with the State's investigation of, analysis of, and response to the incident;
- C. Take all reasonable steps to mitigate any harm caused to affected individuals and/or entities and to prevent any future reoccurrence;
- D. Provide the State with documentation of responsive actions taken related to the disclosure, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement; and
- E. Comply with applicable data breach notification laws, including without limitation the provision of credit monitoring and other fraud prevention measures, for a period of twelve (12) months from the date that Vendor notifies Customer of the Adverse Event.

The State will determine if notification to individuals or entities other than the State is required and if the notification will be carried out by the State or by the Vendor. The method and content of the notification of the affected parties will be subject to approval by the State.

At the State's discretion and at the Vendor's expense the Vendor may be required to use a credit monitoring service, call center, and/or a forensics company.

Notwithstanding any other provision of this agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in the notification, investigation and remediation of the disclosure.

20. BROWSER

The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, Adobe ColdFusion and Adobe Flash will not be used in the system, site, and/or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

21. SECURITY ACKNOWLEDGEMENT FORM

The Vendor will be required to sign the Security Acknowledgement form which is attached to this Agreement as Exhibit C. The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This form constitutes the agreement of Vendor to be responsible and liable for ensuring that the Vendor, Vendor's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy- Contractor Version (ITSP) found at <https://bit.sd.gov/vendor/default.aspx> . Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Vendor does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Vendor's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Vendor and Subcontractor's, Agents, Assigns

and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

22. BACKGROUND CHECKS

The State requires all employee(s) of the Vendor, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo background checks against county and national criminal databases, social security tracing, and Global Watchlist. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Vendor, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its reasonable discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Vendor with notice of this determination.

23. INFORMATION TECHNOLOGY STANDARDS

Any service, software or hardware provided under this agreement will comply with state standards which can be found at <http://bit.sd.gov/standards/>

24. SECURITY

The Vendor shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks. By signing this agreement, the Vendor warrants that all Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:

- A. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
- B. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.

- C. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
- D. **Low**- Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.

Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.

All members of the development team have been successfully trained in secure programming techniques.

- B. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
- C. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at <http://bit.sd.gov/standards/>.
- D. The Vendor will fully support and maintain the Vendor's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Vendor may not withhold support from the State for this application nor charge the State additional fees as a result of the State moving the Vendor's application to a new release of third-party technology if:
 - i. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
 - ii. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Vendor may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.

If a code base or platform on which the Vendor's application depends is no longer supported, maintained, or patched by a qualified third party the Vendor commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Vendor to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

25. MALICIOUS CODE

- A. The Vendor warrants that the service/ licensed software contains no code that does not support an application requirement.
- B. The Vendor warrants that the service/ licensed software contains no malicious code.
- C. The Vendor warrants that the Vendor will not insert into the service/ licensed software or any media on which the service/ licensed software is delivered any malicious or intentionally destructive code.
- D. The Vendor warrants that the Vendor will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the service/ licensed software before installation. In the event any malicious code is discovered in the service/ licensed software delivered by the Vendor, the Vendor shall provide the State at no charge with a copy of the applicable service/ licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

26. LICENSE AGREEMENTS

Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end_users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

27. WEB AND MOBILE APPLICATION

The Vendor's application is required to;

- A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
- B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
- C. close all connections and close the application at the end of processing;
- D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
- E. have no code not required for the functioning of application;
- F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
- G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
- H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
- I. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
- J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application;
- K. access no data outside what is defined in the "About" information for the Vendor's application;
- L. your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;

- M. any website developed for the State and hosted by the State must have a Single Sign On capability with the State's other websites;
- N. if any health or medical information is gathered or accessed by this application that is not protected by HIPAA and HITECH rules and regulations then the opening screen must state, in an easy to read font that the application is gathering and or accessing health and or medical information and the user's privacy is not protected by federal regulations; and
- O. any application to be used on a mobile device must be password protected.

The Vendor is required to disclose all:

- A. functionality;
- B. device and functional dependencies;
- C. third party libraries used;
- D. methods user data is being stored, processed or transmitted;
- E. methods used to notify the user how their data is being stored, processed and or transmitted;
- F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted;
- G. methods used to record the user's response(s) to the notification that their data is being stored, processed and or transmitted;
- H. methods used to secure the data in storage, processing or transmission; and
- I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
- J. methods used to create and customize existing reports;
- K. methods used to integrate with external data sources;
- L. methods used if integrates with public cloud provider;
- M. methods and techniques used and the security features that protect data, if a public cloud provider is used; and
- N. formats the data and information uses.

If the application does not adhere to the requirements given above or the Vendor has unacceptable disclosures, at the State's discretion, the Vendor will rectify the issues at no cost to the State.

28. INTENDED DATA ACCESS METHODS

The Vendor's application will not allow a user, external to the State's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Vendor's application can only access data by methods consistent with the intended business functions. If the State can demonstrate the application flaw, to the State's satisfaction, then the Vendor will rectify the issue, to the State's satisfaction, at no cost to the State.

29. OFFSHORE SERVICES

The Vendor will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

30. VENDOR'S SOFTWARE LICENSES

The Vendor must disclose to the State the license(s) for any third-party software and libraries used by the Vendor's product(s) ((and/or) in the project by the Vendor) covered under this agreement if the State will not be the license(s) holder. The Vendor is required to provide copies of the license(s) for the third-party software and libraries to the State. No additional software and libraries may be added to the project after the contract is signed without notifying the State and providing the licenses of the software and libraries. Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Vendor to fulfil the Vendor's commitments agreed to in this agreement is the responsibility of the Vendor, not the State.

31. VENDOR TRAINING REQUIREMENTS

The Vendor, Vendor's employee(s), and Vendor's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, and v) Security incident response.

32. DATA SANITIZATION

At the end of the project covered by this Agreement the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Vendor and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the State. The only exceptions are when the State Data must be maintained after the project is completed for legal reasons or the State data is on a backup medium where the State data cannot be separated from other data. If the state data cannot be sanitized for these reasons, then the Vendor must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.

This contract clause remains in effect for as long as the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities have the State data, even after the Agreement is terminated or the project is completed.

33. USE OF PORTABLE DEVICES

The Vendor shall prohibit its employees, agents, affiliates, and subcontractors from storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

34. REMOTE ACCESS

The Vendor shall prohibit its employees, agents, affiliates, and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

35. THIRD PARTY HOSTING

If the Vendor has the State's data hosted by another party the Vendor must provide the State, the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the Vendor changes from the Vendor hosting the data to a third-party hosting

the data or changes third-party hosting provider, the Vendor will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

36. SECURING OF DATA

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Vendor warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

37. SECURITY PROCESSES

The Vendor shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing.

38. IMPORT AND EXPORT OF DATA

The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other Vendors.

39. SCANNING AND AUDIT AUTHORIZATION

The Consultant will provide the State at no cost and at a date, time and for duration agreeable to both parties, authorization to scan and access to a test system containing test data for security scanning activities. The system and data provided to the State by Consultant for testing purposes will be considered a test system containing test data. The State will not scan any environment known by the State to be a production environment at the time the scan is performed by the State. Consultant provides their consent for the State or any third-party acting for the State to scan the systems and data provided as the State wishes using any methodology that the State wishes. Any scanning performed by the State will not be considered a violation of any licensure agreements the State has with the Consultant or that the consultant has with a third-party.

The Consultant will also allow the State at the State's expense, not to include Consultant's expenses, to perform up to two security audit and vulnerability assessments per year to provide verification of Consultant's IT security safeguards for the system and its data. The State will

work with the Consultant to arrange the audit at a time least likely to create workload issues for the Consultant and will accept scanning a test or UAT environment on which the code and systems are a mirror image of the production environment.

Scanning by the State or any third-party acting for the State will not be considered reverse engineering. If the State's security scans discover security issues the State may collaborate, at the State's discretion with, the Consultant on remediation efforts. These remediation efforts will not be considered a violation of any licensure agreements between the State and Consultant. In the event of conflicting language this clause supersedes any other language in this, or any other agreement made between the State and the Consultant.

The Consultant agrees to work with the State to rectify any serious security issues revealed by the security audit and or security scanning. This includes additional security audits and security scanning that shall be performed after any remediation efforts to confirm the security issues have been resolved and no further security issues exist. If the Consultant and the State agree that scanning results cannot be achieved that are acceptable to the State, then the State may terminate the Agreement without further obligation.

40. SYSTEM UPGRADES

To the extent possible, advance notice of 30 days shall be provided the State of any major upgrades or system changes the Vendor will be implementing unless the changes are for reasons of security. A major upgrade is a replacement of hardware, software or firmware with a newer or improved version, in order to bring the system up to date or to improve its characteristics. The State reserves the right to postpone these changes unless the upgrades are for security reasons. The State reserves the right to scan the Vendor's systems for vulnerabilities after a system upgrade. These vulnerability scan can include penetration testing of a test system at the State's discretion.

41. PASSWORD PROTECTION

The website(s) and or service(s) that will be hosted by the Vendor for the State will be password protected. If the Vendor provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

42. MOVEMENT OF PROTECTED STATE DATA

Any State data that is protected by Federal or State statute or requirements or by industry standards must be kept secure. When protected State data is moved to any of the Vendor's production or non-production systems, security must be maintained. The Vendor will ensure

that that data will at least have the same level of security as it had on the State's environment. The State's security policies can be found in the Information Technology Security Policies (ITSP).

43. BANNED SERVICES

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

44. MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor and/or the Vendor's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

45. VENDOR ELECTION NOT TO RENEW

The Vendor is obligated to give the State one hundred and eighty (180) days written notice in the event the Vendor intends not to renew the contract or intends to raise any fees or costs associated with the Vendor's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract.

46. DATA LOCATION

The Vendor shall provide its services to the State as well as storage of State data solely from data centers in the continental United States. The Vendor will not allow any State to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall not allow its employees or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access State data remotely only as required to provide technical support or to fulfill the terms of this Agreement. If the State's data being remotely accessed is legally protected data or considered sensitive by the State, then:

- i. The device used must be password protected;
- ii. Multifactor Authentication must be used;
- iii. The data is encrypted to at least AES 256 both in transit and in storage;
- iv. Data is not put onto mobile media;

- v. No non-electronic copies are made of the data;
- vi. The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed;

The State's Data Sanitization policies are to be followed when the data is no longer needed on the device used to access the data remotely.

47. DATA PROTECTION

Protection of personal privacy and data shall be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State's data at any time. To this end, the Vendor shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

- A. The Vendor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
- B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.
- C. The Vendor will not use such data for the Vendor's own benefit and, in particular will not engage in data mining of State's data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

48. INDEPENDENT AUDIT

The Vendor will disclose any independent audits that are performed on any of its systems to the extent there are results that relate to the functionality of the system that may affect the State. The systems included under this requirement are the Vendor's data center. The summary results of such independent audit(s) shall be provided to the State in any event, whether the audit or certification process is successfully completed or not. The summary results of the audit shall also be disclosed if the audit process did not result in a positive outcome. If the State determines it needs to review more than the summary, the State and Vendor will discuss to reach an agreement on how best to proceed with sharing specific detailed analysis that may be confidential.

49. NONDISCLOSURE AND SEPARATION OF DUTIES

The Vendor shall enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State data or the hardware that State data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State's data or the hardware the State's data resides on.

50. BUSINESS CONTINUITY AND DISASTER RECOVERY

The Vendor shall provide a business continuity and disaster recovery plan upon request and ensure that the State's Recovery Time Objective (RTO) of one hour (1) hour and Recovery Point objective (RPO) of twenty four (24) hours is met. For purposes of this contract, a "Disaster" shall mean any unplanned interruption of the operation of or inaccessibility to the Vendor's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Vendor as soon as possible after the State deems a service outage to be a Disaster.

51. STOLEN DATA LIABILITY

In no event shall the Vendor be liable for loss of good will, or for special, indirect, incidental, consequential or punitive damages arising from the state's use of the services of the Vendor, regardless of whether such claim arises in tort or in contract.

If the state's records or other data submitted for processing are lost or damaged as a result of any failure by the Vendor, its employees or agents to exercise reasonable care to prevent such loss or damages the Vendor's liability on account of such loss or damages shall not exceed the reasonable cost of reproducing such records or data. This limitation shall not apply in the event that the records or data cannot be reproduced at reasonable cost.

52. EXTRACTION OF DATA

Upon notice of termination by the Vendor or upon reaching the end of the term, any information stored in repositories not hosted on the State's infrastructure shall be extracted in a format to enable to State to load the information onto\into repositories. If this is not possible, the information metadata, including data structure descriptions and data dictionary, and data will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement, the State again requires that State applications that store information to repositories not hosted on the State's infrastructure require the Vendor, before termination (whether initiated by the State or the Vendor), to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories, the information (metadata (data

structure descriptions) and data) will be extracted into a text file format and returned to the State. Vendor shall be compensated at the rate of \$185 per hour spent on the extraction of data.

53. HOST FACILITY PHYSICAL SECURITY

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate physical security. This includes, at a minimum, centrally administered electronic locks that control entry and exit from all rooms where the hosted system resides. Any door security system must either be connected to the building's power backup system as defined elsewhere or have internal battery power sufficient to last 24 hours in normal usage. Security events for the physical access system must be logged and the logs stored electronically in a secure location in a non-changeable format and must be searchable. Retention on the logs must be not less than 7 years. Log entries must be created for at least: successful entry and exit (indicating whether the access was to enter or exit the room) as well as all security related events such as, doors left open more than 30 seconds, forced entries, failed entry attempts, repeat entries without exit, repeat exits without entry, attempts to access doors for which access was not authorized. The Vendor agrees to provide, at the State's request, full access to search the security logs for any access or security events related to any and all rooms and physical locations hosting the State's system.

54. REDUNDANT POWER AND COOLING TO ALL HARDWARE

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate all facilities supporting the application have adequate redundant power and cooling capacity to operate uninterrupted, and without the need to refuel generators, for not less than 24 hours in the event the local external power fails.

55. UPS BACKUP

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have adequate UPS power to carry the systems for not less than 10 minutes, and to protect the system from power fluctuations including, but not limited to, surge, spikes, sags, and instability.

56. RIGHTS AND LICENSE IN AND TO STATE DATA

The parties agree that between them, all rights including all intellectual property rights in and to State's data shall remain the exclusive property of the State, and that the Vendor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the

purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

57. CESSATION OF BUSINESS

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any State-owned assets and data. The Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

58. SERVICE LEVEL AGREEMENTS

The Vendor warrants that all services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such services. The Vendor further warrants that the services will be operational at least 99.99% of the time in any given month during the term of this Agreement. In the event of a service outage, the Vendor will:

- A. Promptly and at the Vendor's expense, use commercial best efforts to restore the services as soon as possible, and
- B. Unless the outage was caused by a Force Majeure event refund or credit the State, at the State's election, the pro-rated amount of fees corresponding to the time Services were unavailable or \$100 US funds per incident, whichever is the greater amount. For the purpose of this agreement, an incident, regardless of time required to return to online position and whether re-keying of data is necessary to return, is defined as any significant reduction in the availability of hosted services lasting more than one minute or resulting in data loss, rework, or occurring more than 3 times in a 24-hour time period. For example, being forced offline no more than twice in 24 hours would not be an incident if the user could get back online within 60 seconds and continue work where he or she left off. Being forced off-line 3 times in a day would be an incident, regardless. Being forced off-line once in a 24-hour period of

time, however, that resulted in the user having to rekey data that was lost would be an incident. Entering User authentication to log on shall not be considered data entry.

The Vendor will provide the State with seven days prior notice of scheduled downtime in the provision of services for maintenance or upgrades. To the extent possible, the Vendor will schedule downtime during times of ordinarily low use by the State. In the event of unscheduled or unforeseen downtime for any reason, except as otherwise prohibited by law, the Vendor will promptly notify the State and respond promptly to the State's reasonable requests for information regarding the downtime.

59. LEGAL REQUESTS FOR DATA

Except as otherwise expressly prohibited by law, the Vendor will:

- A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State data maintained by the Vendor;
- B. Consult with the State regarding its response;
- C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and
- D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

60. EDISCOVERY

The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

61. DATA RETENTION AND DISPOSAL

- A. Using appropriate and reliable storage media, the Vendor will regularly back up State's data and retain such backup copies for a minimum of 36 months.
- B. The Vendor will retain logs associated with End User activity for a minimum of 7 years unless the parties mutually agree to a different period.

62. MULTI-TENANT ARCHITECTURE LOGICALLY/PHYSICALLY SEPARATED TO ENSURE DATA SECURITY

The Vendor will provide documentation and, at the discretion of the State, allow for on-site inspections as needed to demonstrate that all facilities supporting the application have

adequate safeguards to assure that needed logical and physical separation is in place and enforced to insure data security, physical security, and transport security.

63. ACCESS ATTEMPTS

All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Vendor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

64. PASSWORD POLICIES

Password policies for all Vendor employees will be documented and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multifactor Authentication.

65. ANNUAL RISK ANALYSIS

The Vendor will conduct a risk analysis annually or when there has been a significant system change. The Vendor will provide verification to the State Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

- (i) Penetration testing of the Vendor's system.
- (ii) Security policies and procedures.
- (iii) Disaster recovery plan.
- (iv) Security incident plan.
- (v) Business Associates Agreements.
- (vi) Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the State Contact. The summary will include completion dates for the plan's milestones. Updates on the risk management plan will be sent to the State Contact upon request.

66. WEBSITE PERFORMANCE REPORT

The Vendor will provide to the State reports on the performance of the website being hosted by the Vendor or for the website if hosted by a third party for the Vendor. These reports must be produced by the Vendor on demand. The reports will be in .csv with a mutually agreed to format and at the State's discretion in an unprocessed format. The metrics in the reports will include i) The total number of visits to the website, ii) The average time the website takes to load, and iii) the average length of time a transaction takes on the website.

67. ACCESS TO STATE DATA

Unless this Agreement is terminated, State access to State data amassed under the project covered by this Agreement will not be hindered if there is a:

- i) Contract dispute between the parties to this Agreement.
- ii) There is a billing dispute between the parties to this Agreement.
- iii) The Vendor merges with or is acquired by another company.

The Vendor will also maintain all security requirements of the State as well as any disaster recovery commitments made under this Agreement.

Exhibit C

Security Acknowledgment Form

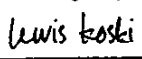
All BIT employees and State contractors must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy")**. Users are responsible for compliance to all information security policies and procedures. *By signature below, the employee or contractor hereby acknowledges and agrees to the following:*

1. Vendor uses non-public State of South Dakota technology infrastructure or information;
2. Vendor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Vendor agrees to follow state and federal regulations in regards to confidentiality and handling of data;
4. Vendor has read and agrees to abide by the Policy;
5. Vendor consents to State contact regarding Policy violations;
6. Vendor shall abide by the policies described as a condition of continued employment / service;
7. Vendor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon departure from the State of South Dakota employment or contract termination;
10. Vendor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends vendors for the State to regularly review the appropriate Policy and annual amendments.

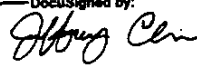
Information Technology Security Policy - BIT: <http://intranet.bit.sd.gov/policies/>
Information Technology Security Policy - CLIENT: <http://intranet.bit.sd.gov/policies/>
Information Technology Security Policy - VENDOR: <http://bit.sd.gov/vendor/default.aspx>

Acknowledgement: State of South Dakota Information Technology Security Policy

Vendor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

DocuSigned by:

E71EASAD2D64D0
Vendor signature

3/18/2022
Date

DocuSigned by:

210DCE98FC94486
BIT Manager or Contact

3/21/2022
Date